Modèles de sécurité réalistes pour la distribution quantique de clés

Aurélien Bocquet

École Doctorale
d'Informatique,
Télécommunications
et Électronique de Paris

Thèse

présentée pour obtenir le grade de docteur

de Télécom ParisTech

Spécialité : Informatique et Réseaux

Aurélien BOCQUET

Modèles de sécurité réalistes pour la distribution quantique de clés.

Soutenue le 6 décembre 2011 devant le jury composé de

Pr Nicolas Cerf	Rapporteurs
Pr Iordanis Kerenidis	
Pr Gérard Cohen	Examinateurs
Pr Thomas Coudreau	
Pr Frédéric Grosshans	
Pr Jean-Pierre Tillich	
Pr Jean-Claude Belfiore	Directeurs de thèse
Pr Romain Alléaume	

À Mai.

Résumé : Depuis son invention en 1984 par C.H. Bennett et G. Brassard, le protocole BB84 a été prouvé sûr contre les attaques les plus générales autorisées par la mécanique quantique, les attaques cohérentes. Cependant, afin de réaliser ces attaques, un adversaire a besoin de mémoire quantique et il n'existe pas à l'heure actuelle de technologie permettant de créer facilement de telles mémoires. Il est donc important de savoir quantifier plus précisément la puissance de l'adversaire lorsque celui-ci n'a pas accès à une mémoire quantique parfaite.

Ces nouveaux modèles de sécurité où la puissance de l'adversaire est limitée par des contraintes plus ou moins fortes sur sa mémoire quantique ont été déjà développés et utilisés pour étudier la sécurité des protocoles réalisant une fonction cryptographique à deux participants (comme la mise en gage de bit quantique par exemple). L'objectif de cette thèse a été d'adapter ces modèles de sécurité à l'étude de la sécurité des protocoles de distribution quantique de clés.

Nous avons ainsi pu étudier la sécurité des principaux protocoles de distribution quantique de clés dans le cas où l'adversaire n'a pas de mémoire quantique et dans un modèle plus général où il est limité par le bruit de sa mémoire. Ces recherches ont permis de mieux comprendre l'influence de la qualité de la mémoire quantique sur la puissance des attaques et ainsi de quantifier le compromis entre la performance d'un protocole (en terme de taux de clé ou de distance atteignable) et la sécurité désirée.

Mots clés : modèle à mémoire bruitée, distribution quantique de clé, attaque optimale, preuve de sécurité, attaque sans mémoire

Abstract : Since its invention in 1984 by C.H. Bennett and G. Brassard, the BB84 protocol has been proven secure against the most general attacks allowed by quantum mechanics, the coherent attacks. In order to conduct such an attack, an eavesdropper needs a quantum memory. It is however technologically very hard to create a quantum memory with adequate properties at the moment. It is therefore useful to study the evolution of the power of the eavesdropper when he doesn't have access to a perfect quantum memory but instead to a noisy quantum memory.

New security models where the power of the eavesdropper is limited by the quality of its quantum memory have already been developed specifically for the study of two-party protocols like bit commitment or oblivious transfer. We therefore used these models and adapted them to the particular case of quantum key distribution.

With these newly developed tools, we have studied the security of quantum key distribution protocols when the adversary doesn't have a quantum memory and when he has access to a limited amount of noisy memory. This research improves our knowledge on the interaction between the quality of the quantum memory and the power of the attacks. It leads to a better understanding of the tradeoff between performance (measured in term of key rate or maximum distance) and security.

Keywords : noisy storage model, optimal memoryless attacks, quantum key distribution, security proof

Table des matières

Introduction

La naissance de l'information quantique

La mécanique quantique est souvent considérée avec la théorie de la relativité comme une des plus grandes avancées scientifiques du XXe siècle. Cette théorie est une description du principe de fonctionnement de l'Univers à une échelle atomique dont l'exactitude a été vérifiée avec une grande précision dans de nombreuses expériences [Odom 2006]. Au delà de l'adéquation remarquable entre les observations expérimentales et ses prédictions, la mécanique quantique a depuis sa création permis le développement de technologies qui ont eu un impact très important sur la vie de tous les jours : des inventions telles que le transistor, le laser ou les systèmes d'imagerie par résonance magnétique nucléaire ont pu voir le jour grâce aux prédictions apportées par le modèle mathématique de la mécanique quantique.

Ce n'est au début des années 70 que la mécanique quantique a été utilisée dans un tout d'autre domaine pour ce qui allait être nommé à la fin des années 90 la théorie de l'information quantique [Nielsen 2000], fruit de la généralisation de la théorie de l'information dans un contexte quantique. Inventée et formalisée par Claude Shannon à la fin des années 40 [Shannon 1949], la théorie de l'information avait déjà révolutionné le domaine des mathématiques appliquées et a permis l'essor des communications numériques et de l'informatique telles que nous les connaissons aujourd'hui avec des applications comme le téléphone cellulaire ou la compression d'image. Cette théorie se limitait par contre à l'origine à une description classique de l'information.

Au sein des nombreux sujets qu'englobe l'information quantique, on peut dater la naissance de la cryptographie quantique au début des années 70 lorsque Stephen Wiesner décrit pour la première fois un protocole permettant la création de billet de banque parfaitement infalsifiables en utilisant les propriétés quantiques des photons [Wiesner 1983]. Ces premiers résultats mettent alors déjà en valeur l'intérêt pratique que peuvent avoir certaines propriétés intrinsèquement quantiques dans le domaine de la cryptographie. On pense notamment au principe d'incertitude d'Heisenberg qui assure de l'impossibilité de mesurer avec une précision infinie deux grandeurs

physiques lorsque leurs observables ne commutent pas, ou au théorème de non clonage qui permet de garantir l'impossibilité de copier parfaitement un état quantique pouvant éventuellement contenir une information secrète. Ces propriétés d'origine quantique resteront les pierres angulaires de tous les protocoles de cryptographie quantique inventés par la suite.

Des applications en cryptographie

C'est le cas par exemple de la distribution quantique de clés, une famille de protocoles permettant la réalisation d'une primitive cryptographique fondamentale : l'établissement d'un secret commun entre deux utilisateurs distants. Ainsi, les propriétés quantiques de la lumière permettent grâce à un protocole bien défini d'assurer une sécurité dite inconditionnelle des clés distribuées. Cela signifie qu'il n'est pas nécessaire d'imposer des contraintes à l'adversaire pour s'assurer de la sécurité du protocole, les seules règles à respecter sont les lois de la mécanique quantique. La promesse d'un niveau absolu de sécurité est une des raisons qui expliquent l'intérêt porté à la cryptographie quantique en général depuis les premiers travaux fondateurs sur le sujet.

Les premiers résultats sur la distribution quantique de clés [Bennett 1984] ont fait espérer des possibilités similaires pour d'autres primitives cryptographiques importantes comme la mise en gage de bit ou la transmission inconsciente dont on savait déjà qu'elles étaient impossibles à réaliser avec une sécurité inconditionnelle dans un cadre classique [Canetti 2006]. Des protocoles implémentant ces primitives et tirant parti des propriétés quantiques de la lumière ont été mis au point mais leur sécurité inconditionnelle a été à chaque fois remise en cause avant qu'on ne découvre au milieu des années 90 qu'il est impossible de réaliser parfaitement ces primitives cryptographiques de manière inconditionnellement sûre même dans un contexte quantique.

Vers de nouveaux modèles de sécurité...

Ces preuves d'impossibilité contre des adversaires non limités ont favorisé par la suite la recherche de nouveaux modèles de sécurité plus restrictifs pour l'adversaire dans lesquels il était possible de prouver la sécurité d'implémentations des primitives cryptographiques concernées par les résultats d'impossibilité. Il a alors été découvert qu'il était possible d'implémenter un protocole de transmission inconsciente sous la condition que l'adversaire ne puisse pas stocker de photons sur de longues périodes et soit limité à des mesures de Von Neumann ou également sous l'unique condition que l'adversaire soit limité à des mesures sur un seul photon à la fois [Mayers 1994] [Crépeau 1994].

Après ces premiers résultats mettant en jeu des restrictions ad hoc, des modèles de sécurité plus généraux ont été élaborés. Ainsi, la sécurité de la plupart des protocoles implémentant une fonction cryptographique à deux participants a pu être prouvée dans le modèle de la mémoire quantique bornée d'abord [Cachin 1998] puis plus tard dans sa généralisation, le modèle de la mémoire bruitée (et bornée) [Wehner 2008].

Plus généralement, ces nouveaux modèles de sécurité où la puissance de l'adversaire est limitée par la qualité de sa mémoire quantique sont intéressants pour plusieurs raisons :

- Compte tenu de l'avancée des recherches dans le domaine des mémoires quantiques [Simon 2010] et de la technologie actuelle ou probablement disponible dans un futur proche, il est raisonnable de supposer qu'un adversaire même doté de moyens considérables ne puissent pas avoir accès à une grande quantité de mémoire quantique très faiblement bruitée.

- La limitation de la qualité de la mémoire quantique d'un adversaire est une hypothèse physique palpable sur laquelle l'incertitude est moins grande que par exemple une supposition de complexité de résolution d'un problème mathématique. Ainsi, une avancée algorithmique sur la factorisation des entiers (qui pourrait menacer par exemple le protocole de chiffrement asymétrique RSA) est moins facilement prédictible que l'amélioration incrémentale des performances des mémoires quantiques en laboratoire.

- Récemment, la sécurité de certains systèmes de distribution quantique de clés a été compromise à cause de défauts d'implémentation de protocoles dont la sécurité inconditionnelle a pourtant été prouvée [Lydersen 2010]. Ainsi, si le maillon faible de la chaîne de sécurité des systèmes de distribution quantique de clés se situe au niveau de l'implémentation plutôt qu'au niveau de la preuve de sécurité, on ne modifie pas beaucoup le niveau de sécurité global du système en utilisant une preuve de sécurité dans un modèle où l'espion est limité par la qualité de sa mémoire quantique tout en optimisant les performances en terme de débit ou de distance atteignable.

... pour la distribution quantique de clés

Au cours de cette thèse, nous avons souhaité étudier la sécurité des protocoles de distribution quantique de clés dans ces nouveaux modèles de sécurité. Contrairement aux protocoles à deux participants mentionnés précédemment, il est possible de créer des protocoles de distribution quantique de clés inconditionnellement sûrs

même contre un adversaire limité par les seules lois de la mécanique quantique. Le choix d'utiliser des modèles de sécurité où l'adversaire est limité par la qualité ou la quantité de la mémoire quantique dont il dispose relève ici d'un compromis entre le niveau de sécurité souhaité et les performances du protocole.

D'un côté, l'utilisation de ces modèles de sécurité fait perdre la propriété de sécurité inconditionnelle autrement atteignable en général pour les protocoles de distribution quantique de clés. Mais comme nous le rappelions au paragraphe précédent, les avancées récentes sur les canaux cachés et la difficulté associée à la fabrication de mémoire quantique confèrent à ce modèle un niveau de sécurité réaliste.

D'un autre côté il est logiquement attendu qu'une diminution des possibilités offertes à l'adversaire par l'intermédiaire de restrictions sur sa mémoire quantique va se traduire par une amélioration des performances des protocoles de distribution quantique de clés en terme de taux d'erreur tolérable ou de taux de clé secrète. Les résultats obtenus dans cette thèse doivent alors permettre de quantifier précisément les bornes de sécurité offertes par ces nouveaux modèles.

Résultats antérieurs et contributions

Les premiers travaux sur les attaques optimales sans mémoire quantique datent des premières études de la sécurité des protocoles de distribution quantique de clés. En effet, les attaques de type interception/réémission (qui ne nécessitent pas l'utilisation de mémoire quantique) ont été étudiées dès l'invention des premiers protocoles de distribution quantique de clés [Bennett 1984] [Bennett 1992a]. Ces attaques étant en général assez facilement analysables, elles constituent souvent la première méthode d'analyse grossière de la sécurité des protocoles. En ce sens ce type d'attaque est utile pour appréhender les spécificités d'un protocole particulier mais elles ne sont pas assez générales pour être les attaques optimales sans mémoire.

Ce cas plus général d'un adversaire limité par l'absence de mémoire quantique a été étudié sur le protocole de distribution quantique de clés BB84 et l'attaque optimale sans mémoire contre ce protocole a pu ainsi être décrite explicitement [Lütkenhaus 1996]. Les travaux effectués au cours de cette thèse permettent entre autre de retrouver ce résultat grâce à une méthode différent. En revanche, à notre connaissance, les attaques optimales sans mémoire contre les protocoles *six-states* et SARG04 n'étaient pas connues avant le travail effectué au cours de cette thèse. Grâce à une optimisation numérique sur l'ensemble des attaques réalisables par l'espion, nous avons pu déterminer explicitement les attaques optimales sans mémoire sur ces trois protocoles.

Concernant le modèle de la mémoire bruitée, il n'existait pas de preuve de sécu-

rité pour les protocoles de distribution quantique de clés avant les résultats obtenus au cours de cette thèse pour les protocoles BB84, *six-states* et SARG04. Notre travail a permis de déterminer précisément les bornes de sécurité concernant ces protocoles de distribution quantique de clés lorsque l'adversaire est limité par le bruit de sa mémoire quantique.

Organisation du manuscrit

Dans le premier chapitre, nous rappelons les principaux concepts de base de la théorie de l'information d'une part et de la mécanique quantique d'autre part pour introduire les outils et les résultats de la théorie de l'information quantique utilisés dans les chapitre suivants.

Dans le deuxième chapitre, nous analysons les modèles de sécurité habituellement utilisés en cryptographie quantique en nous attardant particulièrement sur les protocoles implémentant des fonctions cryptographiques sécurisées à deux participants dont la particularité est d'être impossibles à réaliser avec une sécurité inconditionnelle. Nous présentons alors les nouveaux modèles de sécurité avec un adversaire limité qui ont été développé pour répondre à ce résultat d'impossibilité.

Le troisième chapitre est consacré à l'étude du principe de fonctionnement et des preuves de sécurité de trois protocoles de distribution quantique de clés dont nous étudions la sécurité dans les chapitres suivants : BB84, *six-states* et SARG04. Cela nous permet de justifier notre choix d'étudier la sécurité de ces protocoles dans de nouveaux modèles de sécurité avec un adversaire limité par sa mémoire quantique.

Le quatrième chapitre est consacré à l'étude des attaques optimales contre les protocoles de distribution quantique de clés lorsque l'adversaire n'a pas de mémoire quantique. Nous présentons une nouvelle méthode permettant l'optimisation de l'attaque sur l'ensemble des paramètres accessibles à l'espion pour BB84, *six-states* et SARG04.

Les résultats obtenus dans le chapitre précédent nous permettent enfin dans le cinquième chapitre d'élaborer les preuves de sécurité de ces mêmes protocoles de distribution quantique de clés dans le modèle plus général de la mémoire quantique bruitée. Nous y détaillons en particulier les différentes méthodes employées au cours de la thèse pour borner de plus en plus finement l'information accessible à l'espion et qui aboutissent finalement à une extension du domaine de sécurité des protocoles de distribution quantique de clés étudiés lorsque l'adversaire est limité par le bruit de sa mémoire quantique.

Chapitre 1

Concepts et outils mathématiques

Sommaire

L'objectif de ce chapitre est de décrire les principaux concepts et outils mathématiques nécessaires à la compréhension de cette thèse. La première section est consacrée à la théorie de l'information classique. Dans une deuxième section est présentée une courte introduction à la mécanique quantique. En se basant sur les notions introduites dans ces deux premières parties, nous introduisons les notions d'entropies et de quantités informationnelles dans un cadre quantique dans la troisième section.

Cette introduction ne se voulant pas exhaustive, le lecteur pourra se référer à [Cover 2006] et [Nielsen 2000] pour des informations complémentaires.

1.1 Éléments de théorie de l'information classique

La théorie de l'information classique est un domaine des mathématiques et des communications électroniques qui est né en 1948 lorsque Claude Shannon a publié un article fondateur [Shannon 1948] dans lequel il introduisait notamment les notions d'entropie et de capacité d'un canal. La théorie de l'information est largement basée sur la théorie des probabilités, c'est pourquoi nous rappelons quelques notions importantes de théorie des probabilités dans la première sous-section. Dans les sous-sections suivantes, les notions d'entropie et de codage de canal seront introduites.

1.1.1 Théorie des probabilités discrètes

Cette théorie est une branche des mathématiques dont l'objet est l'analyse des événements aléatoires.

Loi de probabilité. Pour une variable aléatoire discrète notée X qui prend ses valeurs dans $\mathcal{X}$, on note P_X la loi de probabilité associée à X.

Par exemple si on considère le jeu de tirage à pile ou face, on peut alors écrire $\mathcal{X} = \{\text{"pile"}, \text{"face"}\}$ et $P_X[\text{"pile"}] = P_X[\text{"face"}] = \frac{1}{2}$ dans le cas idéal d'une pièce parfaite (non biaisée). Dans ce cas la loi de probabilité associée à X est constante sur l'espace $\mathcal{X}$.

Pour simplifier les notations, on écrit en général $P(X)$ pour désigner la loi de probabilité de X. C'est la notation que nous utiliserons à partir de maintenant dans ce manuscrit. Dans le même souci de simplicité des notations, la probabilité $P(X = x)$ qu'un événement x se produise pourra s'écrire $P(x)$.

L'union de tous les événements de $\mathcal{X}$ est l'événement certain, on a donc la relation $\sum_{x\in\mathcal{X}} P(x) = 1$.

Loi conjointe. La loi conjointe représente la probabilité que deux événements se produisent en même temps. Si X et Y sont deux variables aléatoires alors on écrit de manière équivalente $P(X, Y) = P(XY)$ la loi conjointe de probabilité du couple (X, Y). On peut alors retrouver les lois marginales pour X et Y à partir de cette loi conjointe de la façon suivante :

$$\forall x \in \mathcal{X}, \qquad P(X = x) = \sum_{y\in\mathcal{Y}} P(X = x, Y = y). \tag{1.1}$$

Indépendance. Par définition, on dit de deux variables aléatoires X et Y qu'elles sont indépendantes si la relation suivante est vérifiée :

$$P(XY) = P(X).P(Y). \tag{1.2}$$

Cela signifie que la réalisation d'une de ces variables aléatoires ne modifie pas la loi de probabilité de l'autre.

Probabilité conditionnelle. La loi de probabilité conditionnelle représente la probabilité qu'un événement se réalise sachant qu'un autre événement s'est réalisé. Pour deux variables aléatoire X et Y, la probabilité conditionnelle sur X sachant Y est définie de la façon suivante :

$$\forall (x,y) \in \mathcal{X} \times \mathcal{Y} \text{ tel que } P(y) \neq 0, \qquad P(x|y) \equiv \frac{P(xy)}{P(y)}. \tag{1.3}$$

Pour deux variables aléatoires X et Y indépendantes on peut vérifier facilement que

$$\forall y \in \mathcal{Y}, \qquad P(X|Y=y) = P(X). \tag{1.4}$$

De manière équivalente on a

$$\forall x \in \mathcal{X}, \qquad P(Y|X=x) = P(Y). \tag{1.5}$$

Formules de Bayes. Pour deux variables aléatoires Xet Y, la première formule de Bayes donne une relation entre $P(X|Y)$ et $P(Y|X)$. On a alors

$$\forall (x,y) \in \mathcal{X} \times \mathcal{Y} \text{ tel que } P(x) \neq 0, \qquad P(y|x) = \frac{P(x|y)P(y)}{P(x)}. \tag{1.6}$$

On peut également mentionner ici le théorème des probabilités totales qui permet parfois de calculer plus facilement une probabilité simple en utilisant une probabilité conditionnelle :

$$P(X) = \sum_{y \in \mathcal{Y}} P(X|y)P(y) \tag{1.7}$$

Pour finir nous pouvons aussi mentionner la deuxième formule de Bayes dites de "probabilité des causes" :

$$\forall (x,y) \in \mathcal{X} \times \mathcal{Y} \text{ tel que } P(x) \neq 0, \qquad P(y|x) = \frac{P(x|y)P(y)}{\sum_{y' \in \mathcal{Y}} P(x|y')P(y')}. \tag{1.8}$$

Espérance et variance d'une variable aléatoire. L'espérance d'une variable aléatoire X, notée $\langle X \rangle$ est la valeur moyenne prise par cette variable aléatoire, elle est définie de la façon suivante :

$$\langle X \rangle \equiv \sum_{x \in \mathcal{X}} x.P(x). \tag{1.9}$$

On peut alors définir la variance notée $\mathrm{Var}(X)$ (également noté σ_X^2) d'une variable aléatoire X qui caractérise la dispersion de la loi de probabilité autour de l'espérance de X :

$$\mathrm{Var}(X) = \sigma_X^2 \equiv \left\langle (X - \langle X \rangle)^2 \right\rangle . \tag{1.10}$$

En développant cette formule on trouve la relation

$$\begin{aligned} \sigma_X^2 &= \left\langle X^2 - 2X \langle X \rangle + \langle X \rangle^2 \right\rangle & (1.11) \\ &= \left\langle X^2 \right\rangle - \langle X \rangle^2 . & (1.12) \end{aligned}$$

En l'absence de la connaissance de la loi de probabilité P_X d'une variable aléatoire X, il est tout de même possible d'estimer son espérance en moyennant une grande quantité de réalisations x de cette variable aléatoire. La précision de cette estimation augmente avec le nombre de réalisations : l'erreur tend vers zéro lorsque le nombre de réalisations tend vers l'infini. Mathématiquement ce résultat est connu sous le nom de la loi des grands nombres.

Loi des grands nombres. On considère $X_1, ..., X_n$, un ensemble de n variables indépendantes et identiquement distribuées (iid) et μ leur espérance ($\mu = \langle X_i \rangle$). On définit alors la variable aléatoire Z_n de la façon suivante :

$$Z_n = \frac{1}{n} \sum_{i=1}^{n} X_i. \tag{1.13}$$

La loi faible des grands nombres nous dit que la probabilité que Z_n soit proche de la valeur μ tend vers 1 lorsque n tend vers l'infini. Autrement dit :

$$\forall \varepsilon > 0, \qquad \lim_{n \to \infty} P[|Z_n - \mu| < \varepsilon] = 1. \tag{1.14}$$

Démonstration. Soit $X_1, ..., X_n$, un ensemble de n variables indépendantes et identiquement distribuées d'espérance μ et de variance σ^2. Pour $Z_n = \frac{1}{n} \sum_{i=1}^{n} X_i$ on peut alors calculer :

$$\begin{aligned} \mathrm{Var}(Z_n) &= \frac{1}{n^2} \mathrm{Var}(\sum_{i=1}^{n} X_i) & (1.15) \\ &= \frac{n\sigma^2}{n^2} & (1.16) \\ &= \frac{\sigma^2}{n} & (1.17) \end{aligned}$$

On peut alors appliquer le résultat de l'inégalité de Bienaymé-Tchebychev pour calculer

$$P[|Z_n - \mu| \geq \varepsilon] \leq \frac{\mathrm{Var}(Z_n)}{\varepsilon^2} \leq \frac{\sigma^2}{n\varepsilon^2}. \tag{1.18}$$

On obtient alors la borne

$$P[|Z_n - \mu| < \varepsilon] \geq 1 - \frac{\sigma^2}{n\varepsilon^2} \tag{1.19}$$

qui nous donne le résultat espéré après passage à la limite. □

On peut noter qu'il existe une version plus générale de ce résultat, la loi forte des grands nombres :

$$P[\lim_{n\to\infty} Z_n = \mu] = 1. \tag{1.20}$$

Pour illustrer ce résultat, on peut reprendre l'exemple du jeu de pile ou face. Avec une pièce non biaisée, on aura en moyenne un résultat "pile" 1 fois sur 2. Sur quelques lancés il est très possible de n'avoir que des résultats "pile" et donc d'être loin de la moyenne. Par contre, lorsque le nombre de lancés devient très grand on aura très probablement presque autant de résultats "pile" que de résultats "face". C'est cela qui est exprimé mathématiquement par la loi des grands nombres.

1.1.2 Entropies

Dans cette sous-section nous introduisons les définitions et les principales propriétés de l'entropie, de l'entropie conditionnelle, de l'information mutuelle et enfin des min et max-entropie lissées.

Entropie de Shannon. Si X est une variable aléatoire discrète qui prend ses valeurs dans l'alphabet $\mathcal{X}$ avec une loi de probabilité $P(X)$ alors l'entropie de Shannon de X notée $H(X)$ est définie par la relation suivante :

$$H(X) \equiv -\sum_{x\in\mathcal{X}} P(x) \log P(x), \tag{1.21}$$

où le logarithme est en base 2. Dans le reste du manuscrit les logarithmes seront toujours en base 2 sauf mention contraire. Dans le cas du choix de la base 2, l'unité de l'entropie est le bit.

Sachant que $0 \leq P(x) \leq 1$ on vérifie facilement que $H(X) \geq 0$ pour tout X avec égalité si et seulement si il existe un état $x \in \mathcal{X}$ tel que $P(x) = 1$. Pour la borne supérieure, si on note $n = |\mathcal{X}|$ alors on peut écrire $H(X) \leq \log n$ avec égalité pour une distribution équiprobable.

L'entropie quantifie l'incertitude d'une variable aléatoire. Ainsi l'entropie d'une variable aléatoire qui prend toujours la même valeur est 0. Au contraire dans l'exemple du jeu de "pile" ou "face" l'entropie de la variable aléatoire représentant le résultat est de $\log 2 = 1$ pour une pièce non biaisée.

Il est intéressant d'étudier plus particulièrement l'entropie d'une variable aléatoire dans un alphabet binaire $\mathcal{X} = \{0, 1\}$. En effet cet alphabet est fréquemment utilisé comme support de l'information que ce soit dans le cas classique (on parle alors de bits) ou dans le cas quantique (on parle alors de bits quantiques ou de qubits) qui est présenté plus en détail en section 1.2. Dans ce cas la variable aléatoire X peut être définie de cette façon :

$$X = \begin{cases} 1 & \text{avec probabilité } p \\ 0 & \text{avec probabilité } 1-p \end{cases}. \tag{1.22}$$

Alors a alors :

$$H(X) = -p \log p - (1-p) \log(1-p) = h(p). \tag{1.23}$$

On appelle cette grandeur fonction entropie binaire et on la note $h(.)$. Cette notation sera souvent utile pour simplifier des expressions. Le graphe de cette fonction est donné dans la figure 1.1.

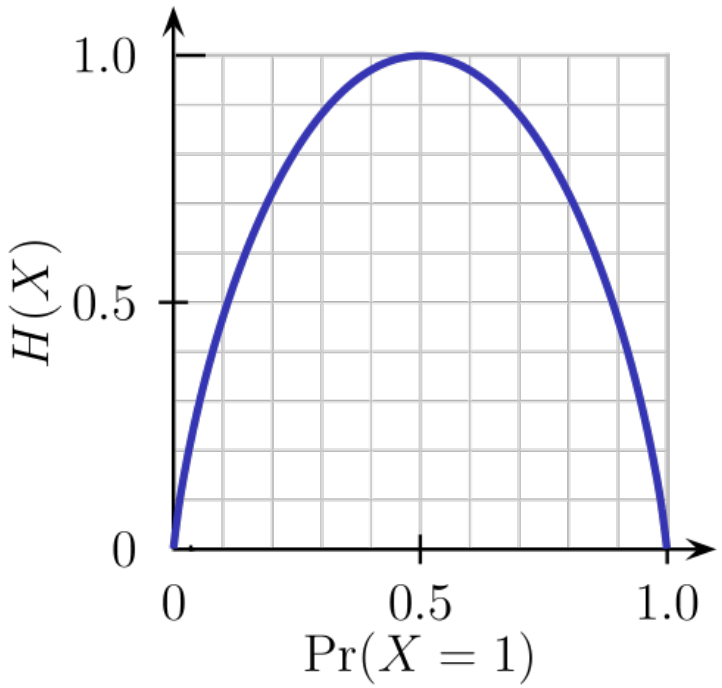


FIGURE 1.1 – Graphe de la fonction entropie binaire $h(.)$.

On peut également définir l'entropie de Shannon pour une paire de variables aléatoires X et Y. Dans ce cas l'entropie conjointe notée $H(X, Y)$ est définie de la façon suivante :

$$H(X, Y) \equiv -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} P(x, y) \log P(x, y) \tag{1.24}$$

Cette entropie conjointe présente plusieurs propriétés qui pourront être utiles par la suite :

- l'entropie conjointe est toujours plus grande que les entropies de Shannon des variables aléatoires séparées : $H(X,Y) \geq H(X)$,
- l'entropie conjointe est toujours positive : $H(X,Y) \geq 0$,
- l'entropie conjointe ne peut pas être plus grande que la somme des entropies des 2 variables aléatoires : $H(X,Y) \leq H(X) + H(Y)$.

Entropies de Rényi. Il existe une généralisation de l'entropie de Shannon appelée entropie de Rényi qui est une famille d'entropies de paramètre α. On note $H_\alpha(X)$ l'alpha entropie de Rényi de la variable aléatoire X. Elle est définie de cette façon :

$$\forall \alpha \geq 0, \alpha \neq 1, \qquad H_\alpha(X) = \frac{1}{1-\alpha} \log \left(\sum_{x \in \mathcal{X}} P(x)^\alpha \right) \tag{1.25}$$

Nous allons nous intéresser plus particulièrement à certaines valeurs de α :

- $\alpha = 1$: il est possible de montrer que l'alpha entropie de Rényi tend vers l'entropie de Shannon lorsque α tend vers 1. L'entropie de Rényi est donc bien une généralisation de l'entropie de Shannon.
- $\alpha = 2$: dans ce cas, l'alpha entropie de Rényi est appelée entropie de collision. En effet on peut calculer $H_2(X) = -\log \left(\sum_{x \in \mathcal{X}} P(x)^2 \right) = -\log P(X = X')$ où X' est une variable aléatoire indépendante de X mais avec la même loi de probabilité.
- $\alpha = 0$: cette entropie en appelée max-entropie et est notée indifféremment $H_0(X)$ ou $H_{\max}(X)$. On peut calculer $H_0(X) = \log |\mathcal{X}|$.
- $\alpha = \infty$: cette entropie est appelée min-entropie et est notée indifféremment $H_\infty(X)$ ou $H_{\min}(X)$. On peut calculer $H_\infty(X) = -\log \max_{x \in \mathcal{X}} P(x)$.

Dans le cas d'une distribution de probabilité X équiprobable on a $H(X) = H_0(X) = H_\infty(X) = \log |\mathcal{X}|$.

La min-entropie, l'entropie et la max-entropie sont reliées par les inégalités

$$H_{\min}(X) \leq H(X) \leq H_{\max}(X) \tag{1.26}$$

avec égalité dans le cas d'une distribution de probabilité uniforme.

Entropie conditionnelle. Lorsque l'on veut quantifier l'incertitude d'une variable aléatoire X sachant que l'on connaît déjà la valeur de la variable aléatoire Y on utilise une quantité appelée entropie conditionnelle de X sachant Y et notée $H(X|Y)$. On la définit de la façon suivante :

$$H(X|Y) \equiv -\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P(x,y)\log P(x|y). \tag{1.27}$$

Cette expression peut être simplifiée de la façon suivante :

$$H(X|Y) \equiv -\sum_{y\in\mathcal{Y}} P(y)H(X|y). \tag{1.28}$$

On peut également définir une entropie conditionnelle pour les min et max-entropies définies auparavant de la façon suivante :

$$H_{\min}(X|Y) = -\log \max_{x\in\mathcal{X},y\in\mathcal{Y}} P(x|y) \tag{1.29}$$

$$H_{\max}(X|Y) = \max_{y\in\mathcal{Y}} \log \left|\{x\in\mathcal{X}/P(x|y)>0\}\right|. \tag{1.30}$$

Les trois entropies conditionnelles que nous venons de définir ne peuvent pas augmenter lorsque qu'on les conditionne à une nouvelle variable aléatoire. Mathématiquement cela se traduit par la relation :

$$\forall\alpha\in\{0,1,\infty\}, \qquad H_\alpha(X|YZ)\leq H_\alpha(X|Y)\leq H_\alpha(X). \tag{1.31}$$

Une autre propriété qui sera utile dans la suite de ce manuscrit est l'additivité de l'entropie conditionnelle (de Shannon). On peut ainsi écrire de manière générale :

$$H(XY|Z) = H(X|Z) + H(Y|XZ). \tag{1.32}$$

Et en particulier lorsqu'on ignore Z on obtient la relation suivante :

$$H(XY) = H(X) + H(Y|X) = H(Y) + H(X|Y). \tag{1.33}$$

Ainsi l'incertitude sur XY est égale à l'incertitude sur X plus l'incertitude sur Y sachant X.

Information mutuelle. L'information mutuelle entre deux variables aléatoires X et Y notée $I(X;Y)$ est une grandeur importante en théorie de l'information dont la définition est la suivante :

$$I(X;Y) = \sum_{x\in\mathcal{X},y\in\mathcal{Y}} P(x,y)\log\frac{P(x,y)}{P(x)P(y)}. \tag{1.34}$$

Avec les définitions données précédemment il est facile de vérifier les relations suivantes :

$$I(X;Y) = H(X) - H(X|Y) \tag{1.35}$$

$$= H(Y) - H(Y|X) \tag{1.36}$$

$$= H(X) + H(Y) - H(XY). \tag{1.37}$$

Comme pour l'entropie, on peut alors définir une information mutuelle conditionnelle :

$$I(X;Y|Z) = H(X|Z) - H(X|YZ). \tag{1.38}$$

Il est important de noter que l'information mutuelle et l'information mutuelle conditionnelle sont symétriques. Mathématiquement cela signifie que $I(X;Y) = I(Y;X)$ et $I(X;Y|Z) = I(Y;X|Z)$.

Min et max-entropie lissées. Telles qu'elles sont définies dans les sections précédentes, les min et max-entropies peuvent être très sensibles à des petits changements de la loi de probabilité des variables aléatoires considérées. Ces variations ne sont pas toujours désirables et il est parfois utile d'avoir recours à une version lissée de ces entropies pour éliminer ces discontinuités. Pour les définir, on introduit une loi conjointe de probabilité Q_{XY} proche de la loi P_{XY}. La définition de la min-entropie ε-lissée est alors :

$$\forall \varepsilon \geq 0, \qquad H_{\min}^{\varepsilon}(X|Y) = \max_{Q_{XY} \in \mathcal{B}^{\varepsilon}(P_{XY})} H_{\min}(X|Y)_{Q_{XY}}, \tag{1.39}$$

où $H_{\min}(X|Y)_{Q_{XY}} = -\log \max_{x \in \mathcal{X}, y \in \mathcal{Y}} Q(x|y)$ et$\mathcal{B}^{\varepsilon}(P_{XY})$ est la boule de rayon ε autour de la loi de probabilité P_{XY}. Au lieu de prendre la valeur de la min-entropie sur un point précis de l'espace de la loi de probabilité, on étend la mesure à une zone ε-proche de ce point pour supprimer les discontinuités.

De la même manière on définit :

$$\forall \varepsilon \geq 0, \qquad H_{\max}^{\varepsilon}(X|Y) = \min_{Q_{XY} \in \mathcal{B}^{\varepsilon}(P_{XY})} H_{\max}(X|Y)_{Q_{XY}}, \tag{1.40}$$

On retrouve les définitions originales de la min-entropie et de la max-entropie en choisissant $\varepsilon = 0$. Le choix de ε permet de régler le degré de lissage souhaité.

1.1.3 Canaux et capacité

Avant d'introduire le deuxième théorème de Shannon sur le codage de canal, nous présentons le modèle du canal BSC (Canal binaire symétrique en anglais).

Canal binaire symétrique. Ce canal discret est très souvent utilisé en théorie de l'information en raison de sa simplicité. On note X et Y les variables aléatoires binaires (donc on le rappelle prenant leur valeur dans l'ensemble $\{0,1\}$) représentant l'information en entrée et en sortie de ce canal. On peut alors paramétrer ce canal par un paramètre de bruit : lors de la transmission d'un bit d'information à travers ce canal, le bit sera inversé avec une probabilité p et restera inchangé avec probabilité $1-p$. Le fonctionnement de ce canal est illustré dans la partie supérieure de la figure 1.2.

Il est facile de calculer les probabilités conditionnelles $P(y|x)$ de ce canal. On obtient $P(Y=0|X=0) = 1-p$ et $P(Y=1|X=0) = p$.

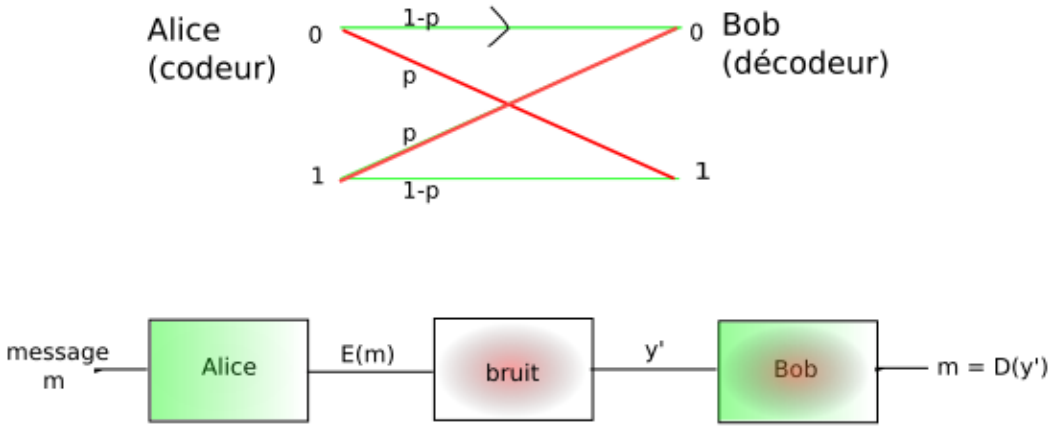


FIGURE 1.2 – Schéma représentant le canal binaire symétrique. "E" y représente l'encodeur et "D" le décodeur.

Codage de canal. Sans précaution particulière, la transmission d'un message à travers ce canal se traduira par une dégradation irréversible de l'information lorsque $p \neq 0$. Pour transmettre de l'information de manière fiable à travers canal, on utilise une technique appelée codage de canal.

Comme cela est illustré dans la partie inférieure de la figure 1.2, pour envoyer un message m à Bob, Alice va encoder son message sous la forme $E(m)$ avant de le transmettre par le canal. Bob de son côté va effectuer l'opération inverse en décodant le message par l'opération $D(y')$.

Il existe de nombreuses familles de code [Richardson 2008] et nous ne les énumèrerons pas ici. Pour illustrer notre propos, nous allons présenter une des techniques de codage les plus simples à mettre en oeuvre, le code à répétition.

Le principe de ce code à répétition est d'envoyer plusieurs fois le même bit d'information pour augmenter les chances de décodage de Bob. La version la plus simple de ce code est la répétition du même bit à trois reprises. Ainsi, lorsque Alice souhaite transmettre le bit "0" elle enverra le mot code "000" dans le canal (et inversement le mot code "111" est envoyé pour le bit "1"). Bob décode ce mot en choisissant le bit présent à 2 ou 3 reprises dans le mot code. Le mot code "001" est par exemple décodé en "0". Il est alors possible de calculer que pour une probabilité d'erreur p dans le canal binaire symétrique, la probabilité que Bob reçoive le mauvais bit est inférieure à p.

Ce code très simple est coûteux puisqu'il faut envoyer 3 bits dans le canal pour

transmettre 1 bit d'information quel que soit le bruit p du canal.

Le deuxième théorème de Shannon présenté dans le paragraphe suivant permet de calculer la quantité maximale d'information transmissible dans un canal.

2e théorème de Shannon Si les variables aléatoires X et Y représentent respectivement l'entrée et la sortie d'un canal sans mémoire alors la capacité C de ce canal est égale à la borne supérieure de l'information mutuelle entre ces 2 variables aléatoires optimisée sur l'ensemble des codes :

$$C = \max_{\text{codes}} I(X;Y). \tag{1.41}$$

En se souvenant des probabilités conditionnelles du canal binaire symétrique données un peu plus haut, on peut alors calculer l'information mutuelle entre X et Y :

$$\begin{aligned} I(X,Y) &= H(Y) - H(Y|X) && (1.42)\\ &= H(Y) - \sum_{x\in\mathcal{X}} P(x)H(Y|x) && (1.43)\\ &= H(Y) - \sum_{x\in\mathcal{X}} P(x)h(p) && (1.44)\\ &= H(Y) - h(p) && (1.45)\\ &\leq 1 - h(p). && (1.46) \end{aligned}$$

Le maximum est atteint lorsque la variable aléatoire Y a une distribution uniforme. Cela se produit lorsque X a également une distribution uniforme. On en déduit alors la valeur de la capacité du canal binaire symétrique :

$$C = 1 - h(p). \tag{1.47}$$

On trouve alors logiquement que pour un paramètre $p = 0.5$ le canal a une capacité nulle alors qu'il a une capacité égale à 1 lorsqu'il n'y a pas d'erreurs.

Le deuxième théorème de Shannon affirme qu'il est toujours possible d'envoyer de l'information à travers un canal de capacité C pourvu que le taux d'envoi R soit inférieur à la capacité. Inversement si il est possible d'envoyer de l'information à travers un canal à un taux R alors la capacité C de ce canal est supérieure ou égale à ce taux.

1.2 Éléments de mécanique quantique

Dans cette partie nous nous attacherons à rappeler les principaux résultats de la mécanique quantique nécessaires à la compréhension de la suite de ce manuscrit.

Pour un cours plus approfondi, le lecteur pourra se référer à [Preskill 2011].

1.2.1 Notations et définitions de base

Un système quantique est un système physique dont l'évolution est régie par la mécanique quantique. L'*état quantique* d'un système est une description complète de celui-ci qui permet de connaître le résultat des expériences que l'on pourrait réaliser. Mais contrairement à la mécanique classique où la connaissance de l'état d'un système permet de prévoir parfaitement le résultat de l'expérience, en mécanique quantique l'état d'un système permet de connaître la distribution de probabilité associées aux différents résultats de mesure possibles : la mécanique quantique est dite non déterministe.

Mathématiquement, un système quantique est représenté par un espace de Hilbert complexe $\mathcal{H}$ de dimension d. La dimension de cet espace de Hilbert dépend du nombre de degrés de liberté du système considéré. Par exemple, pour représenter l'état de polarisation d'un photon, on peut choisir $\mathcal{H} = \mathbb{C}^2$. Dans certains cas, l'espace de Hilbert à considérer est de dimension infinie mais dans cette thèse l'espace de Hilbert sera toujours de dimension finie.

Notation de Dirac. Un vecteur colonne d'un espace de Hilbert $\mathcal{H}$ de dimension d peut être écrit de la façon suivante en notation de Dirac :

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ . \\ . \\ . \\ \psi_n \end{pmatrix}. \tag{1.48}$$

Ce vecteur est appelé un *vecteur-ket* ou tout simplement *ket*. Le vecteur dual associé $\langle\psi|$ est appelé *vecteur-bra* ou simplement *bra* et est donné par :

$$\langle\psi| = \left(\psi_1^*, \ldots, \psi_n^*\right), \tag{1.49}$$

où ψ^* représente le complexe conjugué de ψ.

Le produit scalaire de deux vecteurs-ket $|\psi\rangle$ et $|\phi\rangle$ est un nombre complexe appelé *braket* et noté $\langle\psi|\phi\rangle$:

$$\langle\psi|\phi\rangle = \left(\psi_1^*, \ldots, \psi_n^*\right) \cdot \begin{pmatrix} \psi_1 \\ . \\ . \\ . \\ \psi_n \end{pmatrix} = \sum_{i=1}^{n} \psi_i^* \phi_i^*. \tag{1.50}$$

Ce produit scalaire nous permet alors de définir une norme $\|\cdot\|$ pour l'espace de Hilbert. On a alors $\|\phi\| = \sqrt{\langle\phi|\phi\rangle}$.

Cette notation est aussi utile pour décrire un opérateur linéaire sur l'espace $\mathcal{H}$. Par exemple l'opérateur

$$|\phi\rangle\langle\psi| = \begin{pmatrix} \psi_1 \\ . \\ . \\ . \\ \psi_n \end{pmatrix} \cdot \left(\psi_1^*, \ldots, \psi_n^*\right) \tag{1.51}$$

$$= \begin{pmatrix} \phi_1\psi_1^* & \phi_1\psi_2^* & \ldots & \phi_1\psi_n^* \\ \phi_2\psi_1^* & \phi_2\psi_2^* & \ldots & \phi_2\psi_n^* \\ \ldots & \ldots & \ldots & \ldots \\ \phi_n\psi_1^* & \phi_n\psi_2^* & \ldots & \phi_n\psi_n^* \end{pmatrix} \tag{1.52}$$

est l'opérateur linaire qui au vecteur-ket $|\varphi\rangle$ associe le vecteur-ket $\langle\psi|\varphi\rangle \,.\, |\phi\rangle$.

Cas particulier d'un système de dimension 2. Un bit peut représenter un système dont l'ensemble des états est de taille 2. Par exemple le fait qu'un interrupteur soit sur la position ouverte ou fermée ou qu'une proposition soit vraie ou fausse peut être représenté par un bit. On peut décrire mathématiquement ce bit par un vecteur colonne 2×1. Le bit 0 ou l'état $|0\rangle$ est noté

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \tag{1.53}$$

De même le bit 1 ou l'état $|1\rangle$ est noté

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{1.54}$$

Cette définition est suffisante pour le monde classique mais en mécanique quantique un bit quantique ou qubit est représenté par une matrice

$$|q\rangle = \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} \tag{1.55}$$

où $|q_0|^2 + |q_1|^2 = 1$. On remarque alors qu'un bit classique est un cas particulier de qubit pour lequel une des 2 coordonnées q_0 ou q_1 est nulle. Au lieu de le décrire sous forme de matrice, on peut décomposer le qubit sur la base $\{|0\rangle, |1\rangle\}$ de la façon suivante :

$$|q\rangle = \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} = q_0\,|0\rangle + q_1\,|1\rangle\,. \tag{1.56}$$

Relation de fermeture. Un ensemble de vecteurs $|v_1\rangle, \ldots, |v_n\rangle$ est orthonormal s'ils sont tous orthogonaux entre eux et de norme unité. Un ensemble de n vecteurs orthonormaux dans un espace de dimension n est une base orthonormale de cet espace. Ainsi, n'importe quel vecteur $|\phi\rangle$ peut être décomposé de façon unique sur cette base :

$$|\phi\rangle = \sum_{i=1}^{n} \phi_i |v_i\rangle \tag{1.57}$$

où $\phi_i = \langle v_i|\phi\rangle$ sont les coordonnées du vecteurs $|\phi\rangle$.

En applicant l'opérateur $\sum_{i=1}^{n} |v_i\rangle\langle v_i|$ au vecteur-ket $|\phi\rangle$ on obtient :

$$\sum_{i=1}^{n} |v_i\rangle\langle v_i| \cdot |\phi\rangle = \sum_{i=1}^{n} \phi_i |v_i\rangle = |\phi\rangle . \tag{1.58}$$

On en déduit donc que cet opérateur est l'identité, c'est ce qu'on appelle la relation de fermeture :

$$\sum_{i=1}^{n} |v_i\rangle\langle v_i| = \mathbb{I}_n \tag{1.59}$$

Matrice adjointe. L'adjoint d'une matrice M est la matrice notée $M^\dagger$ obtenue en prenant la matrice transposée de M et en remplaçant chaque coefficient par son complexe conjugué. Autrement dit si $M = [m_{ij}]_{i,j}$ alors $M^\dagger = [\bar{m}_{ji}]_{i,j}$. Une matrice égale à sa matrice adjointe est appelée une matrice hermitienne.

1.2.2 Postulats de la mécanique quantique

Les postulats de la mécanique quantique sont la base de la théorie à partir de laquelle les autres résultats peuvent être déduits.

1er postulat : état quantique. *Un système quantique est parfaitement décrit à l'instant t par un vecteur normalisable $|\phi\rangle$ dans un espace de Hilbert $\mathcal{H}$. Ce vecteur est unique à un facteur de phase près.*

2e postulat : plusieurs particules. *L'espace à considérer pour étudier deux systèmes décrits par les espaces $\mathcal{H}_A$ et $\mathcal{H}_B$ et le produit tensoriel de ces deux espaces $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Si les états des deux systèmes sont les vecteurs $\phi \in \mathcal{H}_A$ et $\psi \in \mathcal{H}_B$ alors le vecteur décrivant le système total est $\Psi = \phi \otimes \psi$.*

Par exemple, étant donnés 2 états $|\phi_A\rangle$ et $|\phi_B\rangle$ l'état total est noté $|\phi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$. En général dans un souci de simplicité le signe $\otimes$ sera omis. On écrira alors simplement $|\phi_A\ \phi_B\rangle$.

3e postulat : évolution. *L'évolution d'un système quantique isolé peut être décrit par une opération unitaire U unique à un facteur de phase près. Cela signifie que l'état $|\phi'\rangle$ d'un système à l'instant t_1 est lié à l'état $|\phi\rangle$ du système à l'instant t_1 par la relation :*

$$\left|\phi'\right\rangle = U\left|\phi\right\rangle. \tag{1.60}$$

Ce postulat a une autre forme connue sous le nom d'équation de Schrödinger qui régit l'évolution temporelle d'un système quantique isolé :

$$i\hbar\frac{\mathrm{d}\left|\phi\right\rangle}{\mathrm{d}t} = \hat{H}\left|\phi\right\rangle, \tag{1.61}$$

avec $\hat{H}$ l'opérateur hamiltonien du système.

4e postulat : mesure. *On peut associer un ensemble d'opérateurs de mesure $\{M_n\}$ à toute mesure effectuée sur un état quantique $|\phi\rangle$ dans un espace $\mathcal{H}$. Ces opérateurs sont indexés par les résultats possibles de la mesure. La probabilité d'obtenir le résultat i lors de la mesure est alors :*

$$P(i) = \left\langle\phi\right| M_i^\dagger M_i\left|\phi\right\rangle. \tag{1.62}$$

La somme des probabilités étant égale à 1, on obtient la relation suivante :

$$\sum_i M_i^\dagger M_i = \mathbb{I}. \tag{1.63}$$

où $\mathbb{I}$ est l'identité. L'état du système après avoir obtenu le résultat i est :

$$\left|\phi'\right\rangle = \frac{M_i\left|\phi\right\rangle}{\sqrt{\left\langle\phi\right| M_i^\dagger M_i\left|\phi\right\rangle}} \tag{1.64}$$

1.2.3 Opérateur densité et propriétés

Opérateur densité. En théorie de l'information quantique on a parfois besoin de considérer un système dont l'état ou l'évolution n'est que partiellement connu. Dans ce cas il est utile d'introduire la notion d'opérateur densité qui permet de décrire l'ensemble des états possibles du système. Après avoir défini cet opérateur densité nous présenterons les principales caractéristiques et propriétés qui nous seront utiles dans le reste de ce manuscrit.

Un opérateur densité ρ sur un espace de Hilbert $\mathcal{H}$ est un opérateur défini positif de norme unité sur $\mathcal{H}$. Autrement dit $\rho \geq 0$ et $\|\rho\| = \mathrm{Tr}(\rho) = 1$.

On note $\mathcal{S}(\mathcal{H})$ l'ensemble des opérateurs densités sur l'espace de Hilbert $\mathcal{H}$.

Un opérateur densité est dit pur si $\rho^2 = \rho$. Dans ce cas l'opérateur peut être écrit sous la forme $\rho = |\phi\rangle\langle\phi|$. Un opérateur densité qui n'est pas pur est dit mixte.

Il existe une base orthonormée $\{|u_i\rangle, \ldots, |u_n\rangle\}$ de vecteurs propres de ρ telle que l'opérateur densité peut s'écrire de la façon suivante :

$$\rho = \sum_{i=1}^{n} P(i) |u_i\rangle\langle u_i| \tag{1.65}$$

où $P(\cdot)$ est la loi de probabilité définie par les valeurs propres de ρ associées aux vecteurs propres $\{|u_i\rangle, \ldots, |u_n\rangle\}$.

Une autre caractérisation d'un opérateur densité pur est qu'une de ses valeurs propre est égale à 1 tandis que les autres sont nulles.

Systèmes à plusieurs particules. Le 2$^{\text{e}}$ postulats de la mécanique quantique peut être exprimé en terme d'opérateurs densité. Étant donnés deux systèmes quantiques représentés par les espaces de Hilbert $\mathcal{H}_A$ et $\mathcal{H}_B$ et dont les états quantiques sont les opérateurs densité $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ et $\rho_B \in \mathcal{S}(\mathcal{H}_B)$ alors le système total est représenté par l'opérateur densité $\rho_{AB} = \rho_A \otimes \rho_B \in \mathcal{S}(\mathcal{H}_{AB})$.

Il est judicieux d'introduire ici des états particuliers d'un système bipartite appelés les états de Bell. Ces états au nombre de 4 sont notés :

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.66}$$

$$\left|\phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{1.67}$$

$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{1.68}$$

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1.69}$$

Trace partielle. Étant donné un système décrit par la matrice densité $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$, l'état du système A (sa matrice densité) est obtenu en faisant la trace partielle sur le système B :

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}), \tag{1.70}$$

où la trace partielle est définie par

$$\mathrm{Tr}_B(|\phi\rangle\langle\phi'| \otimes |\psi\rangle\langle\psi'|) = \mathrm{Tr}(|\psi\rangle\langle\psi'|)\,|\phi\rangle\langle\phi'| = \langle\psi|\psi'\rangle\,|\phi\rangle\langle\phi'|\,. \tag{1.71}$$

La matrice densité obtenue après la trace partielle est appelée matrice densité réduite.

Calculons maintenant la trace partiel d'un des états de Bell définis précédemment. On définit

$$\rho = \left|\phi^+\right\rangle\left\langle\phi^+\right| = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2}. \tag{1.72}$$

Le résultat ρ_1 de la trace partielle sur la partie 2 de ρ est alors :

$$\rho_1 = \mathrm{Tr}_2(\rho) = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{\mathbb{I}_2}{2}. \tag{1.73}$$

Cette matrice densité réduite est un état complètement mixte.

Purification. Toute matrice densité mixte peut être vue comme une partie d'un état pur dans un espace plus grand. Mathématiquement, étant donné $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ alors il existe un opérateur densité pur ρ_{AB} sur un système composite $\mathcal{H}_A \otimes \mathcal{H}_B$ dans lequel la dimension de $\mathcal{H}_B$ est au moins égale au rang de ρ_A tel que

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}). \tag{1.74}$$

Si l'opérateur densité ρ_{AB} est pur alors c'est ce qu'on appelle une purification de l'opérateur ρ_A.

Décomposition de Schmidt. Étant donné $|\phi\rangle_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ un état pur d'un système bipartite AB, alors il existe des états orthonormés $|a_i\rangle \in \mathcal{S}(\mathcal{H}_A)$ et $|b_i\rangle \in \mathcal{S}(\mathcal{H}_B)$ tels que

$$|\phi\rangle_{AB} = \sum_i \lambda_i |a_i\rangle |b_i\rangle , \tag{1.75}$$

où les λ_i sont des nombres réels positifs vérifiant la relation $\sum_i \lambda_i^2 = 1$ et appelés les coefficients de Schmidt.

Mixture d'états purs. Considérons un système A qui peut être préparé dans un état $\rho_A^x \in \mathcal{S}(\mathcal{H}_A)$ aléatoirement en fonction de x avec la loi de probabilité $P(x)$. L'opérateur densité ρ_A qui décrit ce système lorsque la valeur de x est inconnue peut s'écrire :

$$\rho_A = \sum_{x\in\mathcal{X}} P(x)\rho_A^x. \tag{1.76}$$

Par exemple l'opérateur densité

$$\rho = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{1.77}$$

peut être interprété comme l'opérateur densité d'un système qui peut être préparé avec probabilité $\frac{1}{2}$ dans l'état $|0\rangle$ ou $|1\rangle$.

États classiques-quantiques. Lorsqu'une partie d'un système est classique et l'autre quantique, on utilise des états hybrides dits classiques-quantiques pour décrire le système total. C'est par exemple le cas lorsque la partie quantique $\mathcal{H}_A$ d'un système dépend de la réalisation d'une variable aléatoire classique X. Pour décrire ce système on utilise le fait qu'un système classique est un cas particulier de système quantique. On représente alors les différentes valeurs possibles de la variable aléatoire X par des vecteurs orthogonaux entre eux $\{|u_x\rangle\}$ dans un espace de Hilbert $\mathcal{H}_X$.

Si l'on reprend le cas précédent d'un système A qui peut être préparé dans un état $\rho_A^x \in \mathcal{S}(\mathcal{H}_A)$ aléatoirement en fonction de x avec la loi de probabilité $P(x)$ alors on peut décrire l'état du système total de la façon suivante :

$$\rho_{AX} = \sum_{x\in\mathcal{X}} P(x)\rho_A^x \otimes |u_x\rangle\langle u_x| . \tag{1.78}$$

Mesure généralisée. La mesure la plus générale à laquelle peut être soumis un système est celle définie par le 4e postulat de la mécanique quantique déjà évoqué à la partie 1.2.2 page 15. Néanmoins, il est parfois utile d'exprimer ce postulat dans un autre formalisme que celui présenté en premier. Cet outil mathématique est appelé le formalisme POVM (Positive Operator-Valued Measurement).

Si on reprend la définition de la mesure du 4e postulat : on associe un ensemble d'opérateurs de mesure $\{M_n\}$ à toute mesure effectuée sur un état quantique $|\phi\rangle$. On définit alors un ensemble $\{E_n\}$ d'éléments du POVM par la relation

$$E_n = M_n^\dagger M_n. \tag{1.79}$$

Chaque élément E_n est un opérateur hermitien positif et l'ensemble vérifie la relation $\sum_n E_n = \mathbb{I}$. Cette dernière relation peut se comprendre comme le fait que la somme des probabilités des différents résultats de mesure soit égale à l'unité.

Dans ce formalisme, la probabilité d'obtenir le résultat n s'écrit alors :

$$P(n) = \mathrm{Tr}(E_n |\phi\rangle\langle\phi|) \tag{1.80}$$

Ainsi, l'ensemble $\{E_n\}$, appelé le POVM, est suffisant pour obtenir toutes les informations nécessaires sur la distribution de probabilité des résultats de la mesure.

1.2.4 Canaux quantiques

Définition. Un canal quantique $\mathcal{E}$ est une application de l'espace des matrices densité vers l'espace des matrices densité :

$$\mathcal{E} : \mathcal{S}(\mathcal{H}) \longrightarrow \mathcal{S}(\mathcal{H}). \tag{1.81}$$

Cette application est complètement positive [1] , linéaire et conserve la trace ($\mathrm{Tr}\,\mathcal{E}(\rho) = \mathrm{Tr}\,\rho$).

Une telle application peut être représentée à l'aide d'opérateurs de Kraus $\{E_k\}$

$$\mathcal{E} : \mathcal{S}(\mathcal{H}) \longrightarrow \mathcal{S}(\mathcal{H}) \tag{1.82}$$

$$\rho \longmapsto \sum_k E_k \rho E_k^\dagger, \tag{1.83}$$

vérifiant

$$\sum_k E_k^\dagger E_k = \mathbb{I}_n, \qquad n = \dim\mathcal{H}. \tag{1.84}$$

Modélisation de l'évolution d'un système ouvert. L'évolution de la matrice densité ρ d'un système fermé est décrite par une transformation unitaire U. On peut représenter cette évolution sous la forme d'un circuit quantique :

$$\rho_0 \;\text{—}\boxed{U}\text{—}\; U\rho_0 U^\dagger \tag{1.85}$$

Pour décrire l'évolution d'un système ouvert appelé *système principal* de matrice densité ρ_0, on introduit l'*environnement*, de matrice densité ρ_{env} qui avec le *système principal* forment un système fermé. L'évolution de l'ensemble $\{$*système principal* + *environnement*$\}$ est donc décrite par une transformation unitaire U.

On note $\mathcal{E}(\cdot)$ le canal quantique représentant l'interaction avec l'environnement. En général, $\mathcal{E}(\rho_0)$ ne peut pas se déduire de ρ_0 par une opération unitaire. On peut alors représenter l'interaction par le circuit quantique suivant :

$$\begin{array}{l} \rho_0 \\ \rho_{\text{env}} \end{array} \text{—}\boxed{U}\text{—} \begin{array}{l} \mathcal{E}(\rho_0) \\ \\ \end{array} \tag{1.86}$$

L'état du système avant son interaction avec l'environnement est $\rho_0 \otimes \rho_{\text{env}}$. On peut alors calculer $\mathcal{E}(\rho_0)$ grâce à la trace partielle sur l'environnement :

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\text{env}}\left[U(\rho \otimes \rho_{\text{env}})U^\dagger\right] \tag{1.87}$$

On munit l'espace de Hilbert de l'environnement d'une base orthonormale $\{|e_k\rangle\}$ et on suppose sans perte de généralité que l'état initial de l'environnement est un état pur avec $\rho_{\text{env}} = |e_0\rangle\langle e_0|$. Si l'environnement n'est pas dans un état pur, on peut toujours ajouter un système pour le purifier. En reprenant l'équation 1.87 on peut

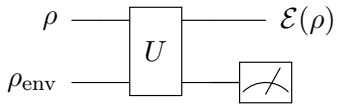
1. On dit d'une application $\mathcal{E}$ qu'elle est complètement positive si l'application $\mathcal{E}\otimes\mathbb{I}_p$ est positive pour tout entier naturel p. On rappelle qu'une application $\mathcal{E}$ est dite positive si $\rho \geq 0 \Rightarrow \mathcal{E}(\rho) \geq 0$

alors écrire :

$$\begin{aligned}
\mathcal{E}(\rho) &= \mathrm{Tr}_{\mathrm{env}}\left[U(\rho\otimes\rho_{\mathrm{env}})U^\dagger\right] && (1.88)\\
&= \sum_k \langle e_k|\, U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger\,|e_k\rangle && (1.89)\\
&= \sum_k \langle e_k|\, U\,|e_0\rangle\,\rho\,\langle e_0|\, U^\dagger\,|e_k\rangle && (1.90)\\
&= \sum_k E_k\rho E_k^\dagger && (1.91)
\end{aligned}$$

où $E_k = \langle e_k| \otimes Id\, U\, |e_0\rangle \otimes Id$ est un opérateur sur l'espace de Hilbert du système principal. Les E_k sont les opérateurs de Kraus de ce canal tels qu'ils ont été définis dans la partie précédente.

Interprétation physique. On suppose qu'on effectue une mesure de l'état de l'environnement dans la base $|e_k\rangle$ après l'interaction. On peut représenter cette opération comme ceci :



(1.92)

L'état du système principal lorsque le résultat de la mesure est k est noté ρ_k. On a alors avant normalisation :

$$\begin{aligned}
\rho_k &\propto \mathrm{Tr}_E\left[|e_k\rangle\langle e_k|\, U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger\,|e_k\rangle\langle e_k|\right] && (1.93)\\
&= \langle e_k|\, U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger\,|e_k\rangle && (1.94)\\
&= E_k\rho E_k^\dagger && (1.95)
\end{aligned}$$

d'où

$$\rho_k = \frac{E_k\rho E_k^\dagger}{\mathrm{Tr}(E_k\rho E_k^\dagger)} \tag{1.96}$$

La probabilité $P(k)$ d'obtenir le résultat k peut se calculer comme :

$$P(k) = \mathrm{Tr}(|e_k\rangle\,\langle e_k|\, U(\rho\otimes|e_0\rangle\,\langle e_0|)U^\dagger\,|e_k\rangle\,\langle e_k|) = \mathrm{tr}(E_k\rho E_k^\dagger) \tag{1.97}$$

Et donc :

$$\mathcal{E}(\rho) = \sum_k P(k)\rho_k = \sum_k E_k\rho E_k^\dagger \tag{1.98}$$

L'action de l'environnement peut être vu comme un bruit qui remplace aléatoirement (avec la probabilité $P(k)$) l'état ρ par l'état ρ_k.

1.2.5 Principaux modèles de canaux quantiques.

Canal à dépolarisation. Le canal à dépolarisation est un modèle de décohérence qui a des propriétés de symétrie remarquables. On peut résumer l'évolution d'un qubit dans ce canal comme ceci : avec probabilité $(1-p)$ le qubit est inchangé, avec probabilité p une erreur apparaît. L'erreur peut être :

1. une inversion de bit : $X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
2. une inversion de phase : $Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
3. les deux à la fois : $Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Mathématiquement ce canal peut s'écrire de la façon suivante :

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}\left(X\rho X + Y\rho Y + Z\rho Z\right) \tag{1.99}$$

où le paramètre p peut prendre n'importe quelle valeur entre 0 et $\frac{3}{4}$. Par un changement de variable, on peut également décrire ce canal par l'équation :

$$\mathcal{E}(\rho) = \frac{p\mathbb{I}}{2} + (1-p)\rho \tag{1.100}$$

où le paramètre p prend des valeurs entre 0 et 1. Dans cette interprétation, le qubit est inchangé avec probabilité $1-p$ et est remplacé par l'état complètement mixte avec probabilité p.

On peut également calculer la décomposition en opérateurs de Kraus de ce canal :

$$\mathcal{E}(\rho) = \sum_{k=0}^{3} E_k \rho E_k^\dagger \tag{1.101}$$

avec

$$E_0 = \sqrt{1-p}\,\mathbb{I} \quad \text{et} \quad E_i = \sqrt{\frac{p}{3}}\,\sigma_i \quad \text{pour} \quad i \in \{1,2,3\} \tag{1.102}$$

Canal à atténuation de phase. Le canal à atténuation de phase est un exemple très intéressant à étudier car il est une bonne approximation de la décohérence ayant lieu dans les systèmes physiques réels. On peut représenter ce canal comme :

$$U: \quad |0\rangle|0\rangle_E \quad \rightarrow \quad \sqrt{1-p}\,|0\rangle|0\rangle_E + \sqrt{p}\,|0\rangle|1\rangle_E \tag{1.103}$$

$$|1\rangle|0\rangle_E \quad \rightarrow \quad \sqrt{1-p}\,|1\rangle|0\rangle_E + \sqrt{p}\,|1\rangle|2\rangle_E \tag{1.104}$$

L'environnement commence ici dans l'état $|0\rangle_E$ et subit une transition avec probabilité p vers l'état $|1\rangle_E$ lorsque le premier qubit est dans l'état $|0\rangle$ ou une transition

vers l'état $|2\rangle_E$ lorsque le premier qubit est dans l'état $|1\rangle$.

En représentation en somme d'opérateurs, on a :

$$\mathcal{E}(\rho) = \sum_{k=0}^{2} E_k \rho E_k^\dagger \tag{1.105}$$

avec

$$E_0 = \sqrt{1-p}\,\mathbb{I},\ E_1 = \sqrt{p}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},\ E_2 = \sqrt{p}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}. \tag{1.106}$$

En développant on obtient :

$$\mathcal{E}(\rho) = (1-p)\rho + p\begin{pmatrix}\rho_{00} & 0\\ 0 & 0\end{pmatrix} + p\begin{pmatrix}0 & 0\\ 0 & \rho_{11}\end{pmatrix} = \begin{pmatrix}\rho_{00} & (1-p)\rho_{01}\\ (1-p)\rho_{10} & \rho_{11}\end{pmatrix} \tag{1.107}$$

Ainsi, on voit que les termes diagonaux restent constants tandis que les autres termes diminuent avec le bruit p.

Pour interpréter physiquement ce canal, on assimile la décohérence introduite par ce canal à un phénomène de dispersion. Si on suppose que la probabilité de dispersion par unité de temps est Γ, de telle façon que la probabilité $p = \Gamma\Delta t$ soit très petite devant 1 au bout d'un temps Δt alors l'évolution des termes non diagonaux au bout d'un temps $t = n\Delta t$ est gouvernée par $(1-p)^n = (1-\Gamma\Delta t)^{t/\Delta t}$ qui devient $e^{-\Gamma t}$ lorsque Δt tend vers 0.

Un état pur $\rho_{\text{pur}} = a\,|0\rangle + b\,|1\rangle$ va donc se transformer en un état diagonal, complètement décohérent $\rho_{\text{dec}} = |a|^2\,|0\rangle\langle 0| + |b|^2\,|1\rangle\langle 1|$ au bout d'un temps $t \gg \Gamma^{-1}$.

Le canal à atténuation d'amplitude. Le canal à atténuation d'amplitude peut se voir comme un modèle du passage d'un système d'un état excité vers un état relaxé. Par exemple un atome se trouvant dans un état excité et retombant dans son état normal après émission d'un photon. On peut représenter ce canal comme :

$$U: \quad |0\rangle|0\rangle_E \ \rightarrow\ |0\rangle|0\rangle_E \tag{1.108}$$

$$|1\rangle|0\rangle_E \ \rightarrow\ \sqrt{1-p}\,|1\rangle|0\rangle_E + \sqrt{p}\,|0\rangle|1\rangle_E \tag{1.109}$$

On suppose que l'atome se trouve initialement dans son état excité $|1\rangle$ et qu'au bout d'un certain temps il soit retombé dans son état normal $|0\rangle$ avec la probabilité p. Ce faisant, l'environnement qui était initialement dans l'état $|0\rangle_E$ reçoit un photon et se retrouve dans l'état $|1\rangle_E$.

En représentation en somme d'opérateurs, on a :

$$\xi(\rho) = \sum_{k=0}^{1} E_k \rho E_k^\dagger \quad \text{avec} \quad E_0 = \begin{pmatrix}1 & 0\\ 0 & \sqrt{1-p}\end{pmatrix},\ E_1 = \begin{pmatrix}0 & \sqrt{p}\\ 0 & 0\end{pmatrix} \tag{1.110}$$

1.3 Entropies et quantités informationnelles dans un cadre quantique

Dans la section 1.1 nous avons rappelé les définitions et les principales propriétés des instruments mathématiques utilisés en théorie de l'information classique. Ensuite dans la section 1.2 nous avons introduit les bases de la mécanique quantique qui nous serviront tout au long de ce manuscrit. Nous pouvons maintenant introduire la notion d'entropie dans un contexte quantique.

1.3.1 Entropie de Von Neumann

L'entropie de Von Neumann est l'équivalent de l'entropie de Shannon dans le monde quantique. Nous allons ici présenter rapidement sa définition ainsi que quelques unes de ses propriétés.

Définition. La motivation derrière le choix de la définition qui va suivre est que l'entropie de Von Neumann d'un état classique soit égale à l'entropie de Shannon de la distribution de probabilité associée. Si $\mathcal{H}_X$ est un espace de Hilbert muni d'une base $\{|e_x\rangle\}$ et que ρ_0 est un état classique de cet espace tel que

$$\rho_0 = \sum_x P(x) \left|e_x\right\rangle \left\langle e_x\right|, \tag{1.111}$$

où $P(\cdot)$ est la loi de probabilité associée à ρ_0 alors on souhaite que :

$$H^{\text{Shannon}}(X) = H^{\text{Von Neumann}}(\rho_0). \tag{1.112}$$

La définition de l'entropie de Von Neumann est la suivante : pour tout état ρ dans un espace de Hilbert $\mathcal{H}$, l'entropie de Von Neumann H de cet état est :

$$H(\rho) \equiv -\operatorname{Tr}(\rho \log \rho). \tag{1.113}$$

Dans cette définition le logarithme est calculé grâce aux valeurs propres de ρ (dont la valeur est entre 0 et 1). En reprenant ρ_0 de l'exemple précédent, on peut calculer :

$$H^{\text{Von Neumann}}(\rho_0) = -\operatorname{Tr}(\rho \log \rho) = -\sum_x P(x) \log P(x) = H^{\text{Shannon}}(X). \tag{1.114}$$

On vérifie bien la coïncidence de l'entropie de Von Neumann avec celle de Shannon.

Un corollaire de cette définition est que l'entropie de Von Neumann d'un état quantique ρ est égale à la minimisation sur toutes les mesures possibles de l'entropie de Shannon des résultats de ces mesures.

Min et max-entropies. De la même façon que précédemment, nous pouvons définir les min et max-entropies quantiques de façon à les rendre compatibles avec la version classique.

Pour tout état ρ dans un espace de Hilbert $\mathcal{H}$:

$$H_{\min}(\rho) \equiv -\log \|\rho\|_\infty, \tag{1.115}$$

où $\|\rho\|_\infty$ est la plus grande valeur propre de ρ. En développant, on obtient

$$H_{\min}(\rho) = -\log \max_x P(x), \tag{1.116}$$

ce qui correspond bien à la définition de la min-entropie classique.

Concernant la max-entropie on a :

$$H_{\max}(\rho) = \log |\sigma(\rho)| \tag{1.117}$$

où $\sigma(\rho)$ est le spectre de ρ (l'ensemble des valeurs propres de ρ) et où $|\sigma(\rho)|$ est le nombre de valeurs propres non nulles de ρ. On retrouve ici aussi le même résultat que pour la max-entropie classique.

Propriétés. Nous avons rassemblé ici quelques propriétés utiles de l'entropie de Von Neumann. Certaines d'entre elles sont inspirées de leur équivalent pour l'entropie classique.

Pour tout opérateur ρ on a :

$$H(\rho) \geq 0, \tag{1.118}$$

et on a égalité si et seulement si ρ est pur.

Cette propriété est directement comparable à la positivité de l'entropie de Shannon. L'entropie classique est nulle lorsque la probabilité d'un des événements est égale à 1.

L'entropie de Von Neumann est maximale lorsque l'état est complètement mixte. Dans ce cas, dans un espace de Hilbert de dimension d, on peut dire :

$$\forall \rho \in \mathcal{H}, \qquad H(\rho) \leq \log d. \tag{1.119}$$

En particulier, pour le cas important d'un espace de Hilbert à 2 dimensions, l'entropie de Von Neumann est comprise entre 0 et 1.

L'entropie est indépendante du choix de la base dans laquelle est décrit l'opérateur. Ainsi on a :

$$H(\rho) = H(U\rho\, U^{-1}). \tag{1.120}$$

L'entropie $H(\rho)$ est une fonction concave. Mathématiquement cela signifie que :

$$H\left(\sum_i \lambda_i \rho_i\right) \geq \sum_i \lambda_i H(\rho_i) \tag{1.121}$$

pour $\{\lambda_i\}$ un ensemble de nombre réels positifs tels que $\sum_i \lambda_i = 1$.

Étant donnés deux espaces de Hilbert $\mathcal{H}_A$ et $\mathcal{H}_B$ et un état pur $\rho_{AB} = |\phi\rangle\langle\phi|$ sur l'espace $\mathcal{S}(\mathcal{H}_{AB})$ alors :

$$H(\rho_A) = H(\rho_B). \tag{1.122}$$

Cela se prouve facilement grâce à la décomposition de Schmidt de l'état ρ_{AB} qui permet d'observer que ρ_A et ρ_B partagent les même valeurs propres et donc la même entropie.

Pour deux états ρ_A et ρ_B quelconques on a

$$H(\rho_A \otimes \rho_B) = H(\rho_A) + H(\rho_B). \tag{1.123}$$

L'entropie dans ce cas est dite additive.

Plus généralement, si ρ_A et ρ_B sont les matrices densités réduites de l'état joint ρ_{AB} alors les inégalités suivantes sont vraies :

$$|H(\rho_A) - H(\rho_B)| \leq H(\rho_{AB}) \leq H(\rho_A) + H(\rho_B). \tag{1.124}$$

La deuxième inégalité est une relation de sous-additivité de l'entropie. L'entropie d'un système bipartite ne peut jamais excéder la somme des entropies des différentes parties du système. Un bon exemple pour illustrer cette inégalité est de considérer un des états de Bell. Cet état pur a une entropie nulle lorsqu'il est considéré dans son ensemble mais chacune de ses parties est un état complètement mixte et donc d'entropie maximale égale à 1.

Concernant les états classiques-quantiques, si ρ_{AX} est un état classique quantique tel que

$$\rho_{AX} = \sum_x P(x) \rho_A^x \otimes |e_x\rangle\langle e_x| , \tag{1.125}$$

alors l'entropie de cet état est

$$H(\rho_{AX}) = H^{\text{Shannon}}(X) + \sum_x P(x) H(\rho_A^x) \tag{1.126}$$

Un résultat important dont la preuve assez longue peut être consultée dans [Nielsen 2000] est le résultat dit de sous-additivité forte. Étant donnés 3 systèmes quantiques A, B et C quelconques alors la relation suivante est vraie :

$$H(ABC) + H(B) \leq H(AB) + H(BC). \tag{1.127}$$

Notations. Nous détaillons ici les notations utilisées dans ce manuscrit concernant l'entropie de Von Neumann. Considérons un opérateur $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ et les opérateurs réduits ρ_A et ρ_B obtenus par l'opération de trace partielle. On peut alors utiliser indifféremment les notations suivantes pour décrire leurs entropies :

$$H(AB)_{\rho_{AB}} = H(\rho_{AB}) = H(AB) \qquad \text{et} \qquad H(A) = H(\rho_A) \tag{1.128}$$

1.3.2 Entropie conditionnelle

De la même manière que pour l'entropie conditionnelle classique, il est possible de définir une entropie conditionnelle dans le cas quantique. On rappelle que dans le cas classique nous avions :

$$H^{\text{Shannon}}(X|Y) = H^{\text{Shannon}}(XY) - H^{\text{Shannon}}(Y). \tag{1.129}$$

Définition. Cette relation nous permet de définir ce que signifie l'entropie conditionnelle dans le cas quantique. Pour deux espaces de Hilbert $\mathcal{H}_A$ et $\mathcal{H}_B$ et une matrice densité $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ alors l'entropie conditionnelle $H(A|B)$ s'écrit :

$$H(A|B) \equiv H(AB) - H(B) = H(\rho_{AB}) - H(\rho_B). \tag{1.130}$$

On pourra aussi retenir cette définition sous une autre forme avec :

$$H(AB) = H(A|B) + H(B). \tag{1.131}$$

Propriétés.

- Si ρ_{AB} est un état pur sur l'espace de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B$ alors $H(A|B) < 0$ si et seulement si ρ_{AB} n'est pas séparable (est intriqué).

Démonstration. Comme ρ_{AB} est un état pur, on a $H(AB) = 0$. Ainsi on peut écrire $H(A|B) = H(AB) - H(B) = -H(B)$. On a donc

$$\begin{aligned} H(A|B) < 0 &\iff H(B) > 0 && (1.132)\\ &\iff \rho_B = \mathrm{Tr}_A(\rho_{AB}) \text{ n'est pas un état pur} && (1.133)\\ &\iff \rho_{AB} \text{ n'est pas séparable} && (1.134) \end{aligned}$$

□

Une conséquence de cette propriété est que l'entropie conditionnelle quantique peut être négative.

- Si $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ est un état *pur* alors

$$H(A|B) = -H(A|C). \tag{1.135}$$

Démonstration. On se souvient en effet que pour un état ρ_{ABC} pur on a $H(AB) = H(C)$ et $H(B) = H(AC)$, en développant l'entropie conditionnelle on peut écrire

$$H(A|B) = H(AB) - H(B) = H(C) - H(AC) = -H(A|C). \tag{1.136}$$

□

- Concernant les états classiques-quantiques, pour une matrice densité $\rho_{AX} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_X)$ classique sur X telle que

$$\rho_{AX} = \sum_x P(x)\rho_A^x \otimes |e_x\rangle\langle e_x|, \tag{1.137}$$

l'écriture de l'entropie conditionnelle se simplifie sous la forme

$$H(A|X) = \sum_x P(x)H(\rho_A^x). \tag{1.138}$$

En effet, en appliquant la définition de l'entropie conditionnelle et en se souvenant du résultat 1.126 on obtient :

$$\begin{aligned} H(A|X) &= H(AX) - H(X) && (1.139)\\ &= H(X) + \sum_x P(x)H(\rho_A^x) - H(X) && (1.140)\\ &= \sum_x P(x)H(\rho_A^x). && (1.141) \end{aligned}$$

On remarque également que pour un état classique-quantique on a $H(A|X) \geq 0$.

- On peut reformuler le résultat de sous-additivité forte obtenu précédemment (1.127) grâce aux entropies conditionnelles. Ainsi pour tout état $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ on a

$$H(A|B) \geq H(A|BC). \tag{1.142}$$

Ce résultat est assez facile à comprendre lorsqu'il est formulé sous cette forme. En effet cela revient à dire que l'incertitude sur le système A ne peut qu'augmenter lorsqu'on retire l'information C. Au pire le système C n'apportait pas d'information sur le système A, dans ce cas on a égalité.

- Une borne supérieure sur l'entropie conditionnelle d'un opérateur densité peut être obtenue facilement en observant que $H(A|B) \leq H(A)$. Ainsi pour un espace de Hilbert de dimension d on a

$$H(A|B) \leq \log d. \tag{1.143}$$

1.3.3 Information mutuelle

L'information mutuelle quantique est définie de manière similaire à l'information mutuelle classique. Ainsi pour un état $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ on appelle information mutuelle entre A et B la quantité $I(A : B)$ définie par

$$I(A : B) \equiv H(A) + H(B) - H(AB) = H(A) - H(A|B). \tag{1.144}$$

Information mutuelle conditionnelle. On peut aussi définir une information mutuelle conditionnelle de la façon suivante : pour $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ un opérateur densité quelconque,

$$I(A:B|C) = H(A|C) - H(A|BC). \tag{1.145}$$

L'information mutuelle ainsi définie a la particularité d'être toujours positive.

1.3.4 Min et max-entropie

Le lecteur pourra trouver les démonstrations de la plupart des propriétés énoncées dans [Renner 2005a].

Définition de la min- et max-entropie. Pour un état $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ et un état $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$ on définit la min-entropie de ρ_{AB} par rapport à σ_B de la façon suivante :

$$H_{\min}(\rho_{AB}|\sigma_B) \equiv -\log \lambda, \tag{1.146}$$

où λ est le plus petit nombre réel tel que tous les coefficients de la matrice $(\lambda\ \mathrm{id}_A \otimes \sigma_B - \rho_{AB})$ soient positifs ou nuls.

On peut également définir la max-entropie de ρ_{AB} par rapport à σ_B :

$$H_{\max}(\rho_{AB}|\sigma_B) \equiv \log \mathrm{Tr}\left((\mathrm{id}_A \otimes \sigma_B)\Pi_{\rho_{AB}}\right), \tag{1.147}$$

où $\Pi_{\rho_{AB}}$ est le projecteur sur le support de ρ_{AB}.

On définit alors les min- et max-entropies de ρ_{AB} par rapport à l'espace de Hilbert $\mathcal{H}_B$:

$$H_{\min}(\rho_{AB}|B) \equiv \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B) \tag{1.148}$$

$$H_{\max}(\rho_{AB}|B) \equiv \sup_{\sigma_B} H_{\max}(\rho_{AB}|\sigma_B). \tag{1.149}$$

Dans le cas où l'espace $\mathcal{H}_B$ est l'espace trivial $\mathbb{C}$ alors on a

$$H_{\min}(\rho_{AB}|B) = H_{\min}(\rho_A) = -\log \lambda_{\max}(\rho_A), \tag{1.150}$$

$$H_{\max}(\rho_{AB}|B) = H_{\max}(\rho_A) = \log \mathrm{rg}(\rho_A). \tag{1.151}$$

Propriétés. Pour un état $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ et un état $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$ l'inégalité suivante est toujours vérifiée :

$$H_{\min}(\rho_{AB}|\sigma_B) \leq H_{\max}(\rho_{AB}|\sigma_B). \tag{1.152}$$

La max-entropie est toujours plus grande que la min-entropie.

Additivité. La min- et max-entropie de deux systèmes indépendants est égale à la somme des entropies des deux systèmes. Ainsi on a :

$$H_{\min}(\rho_{AB} \otimes \rho_{A'B'}|BB') = H_{\min}(\rho_{AB}|B) + H_{\min}(\rho_{A'B'}|B') \tag{1.153}$$
$$H_{\max}(\rho_{AB} \otimes \rho_{A'B'}|BB') = H_{\max}(\rho_{AB}|B) + H_{\max}(\rho_{A'B'}|B') \tag{1.154}$$

Sous-additivité. Pour un état $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ et un état $\sigma_{BC} \in \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_C)$ on a les inégalités suivantes :

$$H_{\min}(\rho_{ABC}|\sigma_{BC}) \leq H_{\min}(\rho_{AB}|\sigma_B) \tag{1.155}$$
$$H_{\max}(\rho_{ABC}|\sigma_{BC}) \leq H_{\max}(\rho_{AB}|\sigma_B). \tag{1.156}$$

États classiques-quantiques. Pour un état $\rho_{ABX} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_X)$ et un état $\sigma_{BX} \in \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_X)$ classiques sur X alors on a :

$$H_{\min}(\rho_{ABX}|\sigma_{BX}) = \inf_{x \in \mathcal{X}} H_{\min}(\rho^x_{AB}|\sigma^x_B) \tag{1.157}$$
$$H_{\max}(\rho_{ABX}|\sigma_{BX}) = \log \sum_{x \in \mathcal{X}} 2^{H_{\max}(\rho^x_{AB}|\sigma^x_B)}. \tag{1.158}$$

Cette égalité permet de calculer les entropies sur les états classiques-quantiques à partir des entropies des états quantiques.

Règle de chaînage. Pour un état $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ on a :

$$H_{\min}(\rho_{ABC}|C) \leq H_{\min}(\rho_{ABC}|BC) + H_{\max}(\rho_B). \tag{1.159}$$

Cette règle sera très utile par la suite, surtout dans sa version lissée.

Action d'un canal quantique. Pour un état $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, un état $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$, un état $\sigma'_B \in \mathcal{S}(\mathcal{H}'_B)$ et un canal quantique $\mathcal{E}$ on a :

$$H_{\min}(\rho_{A'B'}|\sigma'_B) \geq H_{\min}(\rho_{AB}|\sigma_B), \tag{1.160}$$

où $\rho_{A'B'} = \mathcal{E}(\rho_{AB})$. Cela signifie concrètement que la min-entropie ne peut qu'augmenter sous l'action d'un canal quantique.

Définition des entropies lissées. Il est parfois nécessaire d'avoir recours à des versions lissées des min- et max-entropies définies précédemment. En effet, telles qu'elles sont définies dans la section précédentes ces entropies ne sont pas continues par rapport à une petite modification du système. Afin de pallier à cet inconvénient nous allons introduire ici les min- et max-entropies lissées.

Pour un état $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, un état $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$ et un paramètre de lissage $\varepsilon \geq 0$ on peut définir la min-entropie ε-lisse et la max-entropie ε-lisse :

$$H^\varepsilon_{\min}(\rho_{AB}|\sigma_B) \equiv \sup_{\bar{\rho}_{AB}} H_{\min}(\bar{\rho}_{AB}|\sigma_B) \tag{1.161}$$
$$H^\varepsilon_{\max}(\rho_{AB}|\sigma_B) \equiv \inf_{\bar{\rho}_{AB}} H_{\max}(\bar{\rho}_{AB}|\sigma_B), \tag{1.162}$$

où les bornes supérieures et inférieures sont prises sur une boule centrée sur ρ_{AB} et de rayon ε au sens de la distance trace $\delta(\rho,\sigma) = \frac{1}{2}\|\rho - \sigma\|_1$.

On peut définir les min- et max-entropies lissées par rapport à l'espace de Hilbert B de la façon suivante :

$$H_{\min}^{\varepsilon}(\rho_{AB}|B) \equiv \sup_{\sigma_B} H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B) \tag{1.163}$$

$$H_{\max}^{\varepsilon}(\rho_{AB}|B) \equiv \sup_{\sigma_B} H_{\max}^{\varepsilon}(\rho_{AB}|\sigma_B). \tag{1.164}$$

Propriétés. La min-entropie lissée de deux systèmes indépendants est plus grande que la somme des min-entropies lissées des deux systèmes. Ainsi on a :

$$H_{\min}^{\varepsilon+\varepsilon'}(\rho_{AB}\otimes\rho_{A'B'}|BB') \geq H_{\min}^{\varepsilon}(\rho_{AB}|B) + H_{\min}^{\varepsilon'}(\rho_{A'B'}|B') \tag{1.165}$$

Comme pour sa version non lissée, on peut généraliser la sous-additivité à la min-entropie lissée :

$$H_{\min}^{\varepsilon}(\rho_{ABC}|\sigma_{BC}) \leq H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B). \tag{1.166}$$

Concernant les états classiques-quantiques, on a maintenant l'inégalité suivante :

$$H_{\min}^{\varepsilon}(\rho_{ABX}|\sigma_{BX}) \geq \inf_{x\in\mathcal{X}} H_{\min}^{\varepsilon}(\rho_{AB}^{x}|\sigma_B^{x}). \tag{1.167}$$

On rappelle également la règle de chaînage pour la min-entropie lissée :

$$H_{\min}^{\varepsilon}(\rho_{ABC}|C) \leq H_{\min}^{\varepsilon}(\rho_{ABC}|BC) + H_{\max}(\rho_B). \tag{1.168}$$

1.3.5 Communication sur un canal quantique

Que la transmission se fasse uniquement entre deux participants légitimes ou en présence d'un espion, il est important de connaître la quantité d'information que peut transmettre un canal quantique donné. En particulier il est parfois utile de calculer la quantité maximale d'information classique qu'un canal quantique est capable de transmettre. Cette valeur limite est appelée la borne d'Holevo.

Borne d'Holevo. On suppose une communication entre Alice et Bob sur un canal quantique. Alice envoie l'état ρ^x avec une probabilité $P(x)$ et Bob mesure l'état grâce à un POVM. Il est alors possible de borner l'information mutuelle entre la variable aléatoire X et la variable aléatoire Y représentant le résultat de la mesure de Bob. On a alors la borne suivante :

$$I(X:Y) \leq H(\rho) - \sum_{x\in\mathcal{X}} P(x)H(\rho^x) \tag{1.169}$$

où $\rho = \sum_{x\in\mathcal{X}} P(x)\rho^x$. Cette valeur limite est appelée quantité de Holevo et est notée $\chi(X:Y)$.

Lien avec la min-entropie. Nous reprenons ici un résultat de [Koenig 2008] sur la signification de la min-entropie dans le cas d'un état classique-quantique.

La situation est la suivante : on considère un état classique-quantique ρ_{XA} et on souhaite obtenir le maximum d'information sur la variable aléatoire X sachant qu'on peut effectuer une mesure sur le système quantique A. Si on note

$$\rho_{XA} = \sum_x P(x) \left|e_x\right\rangle \left\langle e_x\right| \otimes \rho_A^x, \tag{1.170}$$

on peut paramétrer la stratégie par un POVM d'éléments $\{E_x\}$ donnant les résultats x. La probabilité de deviner la valeur de x grâce au système A est alors

$$p^{\text{dev.}}_{\{E_x\}}(X|A) = \sum_{x\in\mathcal{X}} P(x) \operatorname{Tr}(E_x \rho_A^x). \tag{1.171}$$

On peut alors définir la probabilité de réussite comme la maximisation sur tous les POVMs de la probabilité $p^{\text{dev.}}_{\{E_x\}}(X|A)$. On a alors

$$p^{\text{réus.}}(X|A) = \max_{\{E_x\}} p^{\text{dev.}}_{\{E_x\}}(X|A) \tag{1.172}$$

Il est alors possible de démontrer [Koenig 2008] la relation

$$H_{\min}(\rho_{XA}|A) = -\log p^{\text{réus.}}(X|A) \tag{1.173}$$

Chapitre 2

Génèse et analyse des modèles de sécurité utilisés en cryptographie quantique

Sommaire

La cryptographie quantique est un vaste sujet qu'on a parfois tendance à réduire à l'une de ses composantes les plus visibles, la distribution quantique de clés. Pourtant, comme nous allons le voir dans la suite, des primitives cryptographiques telles le tirage à pile ou face ont été étudiées avant même la découverte des premiers protocoles de distribution quantique de clés. De même, l'étude des protocoles à deux participants [1] telles que la mise en gage de bit ou la transmission inconsciente a participé à la création des nouveaux modèles de sécurité que sont le modèle de la

1. protocoles implémentant des fonctions cryptographique à deux participants

mémoire bornée ou celui de la mémoire bruitée.

Dans ce chapitre, nous commencerons par rappeler les principales raisons qui ont amené la communauté scientifique à étudier l'utilisation des phénomènes quantiques en cryptographie. Ce faisant, nous étudierons les protocoles à 2 participants et nous expliquerons pourquoi aucune implémentation même quantique des ces protocoles ne peut être inconditionnellement sûre. Enfin, nous présenterons dans une dernière section les nouveaux modèles de sécurité (dans lesquels la sécurité de la plupart des protocoles à 2 participants peut être prouvée) qui sont apparus en réponse à ce résultat d'impossibilité.

2.1 L'apport de la mécanique quantique en cryptographie

Comme nous allons le voir dans les sous-sections suivantes, les propriétés très particulières de la mécanique quantique rappelées dans le chapitre précédent peuvent assez logiquement être utilisées pour des applications cryptographiques. Nous présentons ici deux des principes importants de la mécanique quantique qui jouent un rôle crucial en cryptographie : le théorème de non clonage et le principe d'incertitude d'Heisenberg.

2.1.1 Idées fondatrices

Principe d'incertitude d'Heisenberg. Le principe d'incertitude d'Heisenberg assure qu'il n'est pas possible d'obtenir simultanément et avec autant de précision que voulue une information sur deux grandeurs telles que la quantité de mouvement et la position d'une particule. Il est par exemple possible de mesurer avec une infinie précision la position d'une particule à un instant donné, mais dans ce cas aucune information ne peut être obtenue sur la quantité de mouvement de cette particule et inversement.

Pour illustrer ce principe, on peut considérer la diffraction de la lumière à travers un orifice de diamètre comparable à la longueur d'onde de la lumière considérée. Les lois de l'optique nous assurent qu'à la sortie de cet orifice la lumière va être diffusée dans toutes les directions. On peut expliquer ce phénomène en utilisant les outils classiques de la mécanique ondulatoire : le principe de Huygens-Fresnel nous permet de calculer les équations qui régissent le problème considéré. Mais si on considère la lumière comme un flux de photons, c'est le principe d'incertitude qui permet alors d'expliquer le phénomène. En effet, faire passer un photon à travers un trou de petit diamètre, c'est en fait connaître sa position à un instant donné avec une grande précision. Le principe d'incertitude d'Heisenberg nous assure que la quantité de mouvement de ce photon (et en particulier sa direction de propagation) n'est pas connue précisément. Plus le trou est petit, moins on connaît la direction de propa-

gation du photon. Cela se traduit par le phénomène de diffraction de la lumière.

Mathématiquement, si on désigne par Δx et Δp les incertitudes sur la position et la quantité de mouvement d'une particule, la relation d'incertitude est habituellement exprimée de la façon suivante :

$$\Delta x \Delta p \geq \frac{\hbar}{2} \tag{2.1}$$

où $\hbar = \frac{h}{2\pi}$ est la constante de Planck réduite.

Plus généralement, pour deux observables P et Q et un état quantique $|\phi\rangle$ quelconque, on a

$$\Delta P \Delta Q \geq \frac{|\langle\phi| [P,Q] |\phi\rangle|}{2} \tag{2.2}$$

où $[P,Q] = PQ - QP$ est le commutateur de P et Q.

Démonstration. On considère deux opérateurs hermitiens A et B et un état quantique $|\phi\rangle$ quelconque. En développant le commutateur de A et B on obtient

$$\begin{aligned} |\langle\phi| [A,B] |\phi\rangle|^2 &= |\langle\phi| AB |\phi\rangle - \langle\phi| BA |\phi\rangle|^2 && (2.3)\\ &= |\langle\phi| AB |\phi\rangle - (\langle\phi| AB |\phi\rangle)^*|^2 && (2.4)\\ &= 4\, \Im(\langle\phi| AB |\phi\rangle)^2 && (2.5) \end{aligned}$$

où $\Im(u)$ est la partie imaginaire de u.

En développant l'anti-commutateur $\{A,B\} = AB + BA$ de A et B on obtient de manière similaire

$$|\langle\phi| \{A,B\} |\phi\rangle|^2 = 4\, \Re(\langle\phi| AB |\phi\rangle)^2. \tag{2.6}$$

où $\Re(u)$ est la partie imaginaire de u.

En rassemblant ces deux résultats on obtient l'égalité

$$|\langle\phi| [A,B] |\phi\rangle|^2 + |\langle\phi| \{A,B\} |\phi\rangle|^2 = 4\, |\langle\phi| AB |\phi\rangle|^2 . \tag{2.7}$$

Or d'après l'inégalité de Cauchy-Schwarz on a

$$|\langle\phi| AB |\phi\rangle|^2 \leq \langle\phi| A^2 |\phi\rangle \langle\phi| B^2 |\phi\rangle . \tag{2.8}$$

En combinant ces deux derniers résultats on peut donc écrire

$$|\langle\phi|\,[A,B]\,|\phi\rangle|^2 \leq 4\,\langle\phi|\,A^2\,|\phi\rangle\,\langle\phi|\,B^2\,|\phi\rangle\,. \tag{2.9}$$

En substituant A et B dans cette équation par $A = P - \langle P\rangle$ et $B = Q - \langle Q\rangle$ où P et Q sont deux observables quelconques on trouve l'inégalité

$$\Delta P \Delta Q \geq \frac{|\langle\phi|\,[P,Q]\,|\phi\rangle|}{2} \tag{2.10}$$

où $\Delta X = \sqrt{\langle X^2\rangle - \langle X\rangle^2}$. □

Dans les protocoles de cryptographie quantique en général, si on considère un photon dont la polarisation peut être fixée à 0°, 45°, 90°ou 135° alors le principe d'incertitude nous assure qu'un observateur malveillant (espion ou participant malhonnête) ne peut pas mesurer sans erreur l'état de polarisation de ce photon. En effet, les observables associées aux mesures dans chacune des bases $\{0^\circ, 90^\circ\}$ ou $\{45^\circ, 135^\circ\}$ ne commutent pas.

Dans les protocoles de distribution quantique de clés, cela permet de s'assurer qu'un espion commet nécessairement des erreurs en tentant de compromettre les communications. Ces erreurs peuvent alors être détectées pendant l'exécution du protocole et les participants honnêtes peuvent alors décider d'abandonner la procédure en cas de taux d'erreur excessif.

Théorème de non clonage

Ce principe très connu de la mécanique quantique a été démontré en 1982 par W.K. Wootters et W.H. Zurek [Wootters 1982]. Il stipule qu'il est impossible de créer une copie parfaite d'un état quantique inconnu.

Si le clonage était possible, le résultat précédent sur le principe d'incertitude d'Heisenberg pourrait être contourné. En effet, pour mesurer parfaitement la position et l'impulsion d'une particule il suffirait de cloner cette particule et de mesurer séparément sur chaque clone la position et l'impulsion avec une précision aussi grande que possible, cette méthode permettant ainsi de violer le principe d'incertitude.

Il est possible de démontrer ce théorème de non clonage par l'absurde en supposant l'existence d'une machine capable de cloner des états quantiques quelconques et d'aboutir finalement à une contradiction.

Démonstration. On suppose qu'il existe un système de clonage qui à partir d'un état $|\phi\rangle$ quelconque et d'un système auxiliaire initialement dans l'état $|0\rangle$ donne l'état $|\phi\rangle \otimes |\phi\rangle$. Ce système est représenté par l'opération unitaire U et on peut écrire :

$$\forall |\phi\rangle \qquad U |\phi\rangle |0\rangle = |\phi\rangle |\phi\rangle . \tag{2.11}$$

On considère alors 2 états quantiques $|\phi\rangle$ et $|\varphi\rangle$. Étant donné qu'une opération unitaire conserve le produit scalaire, on peut écrire

$$\langle 0| \langle \varphi| U^\dagger U |\phi\rangle |0\rangle = \langle \varphi| \langle \varphi| |\phi\rangle |\phi\rangle . \tag{2.12}$$

Et donc finalement on a

$$\langle \phi|\varphi\rangle = (\langle \phi|\varphi\rangle)^2. \tag{2.13}$$

Cette relation n'est vérifiée que si le produit scalaire vaut 0 ou 1, c'est à dire si les états $|\phi\rangle$ et $|\varphi\rangle$ sont orthogonaux ou égaux. Cela n'est pas vrai en général, il y a donc contradiction.

□

Il est donc impossible de créer une machine capable de cloner un état quantique arbitraire. Il est par contre possible de créer une machine capable de cloner une particule qui peut se trouver dans deux états quantiques orthogonaux.

En cryptographie, ce principe permet de s'assurer qu'un éventuel espion ne peut pas simplement copier parfaitement un état quantique voyageant entre deux correspondants. On est assuré que pour récupérer de l'information, cet espion doit nécessairement perturber l'état qu'il cherche à espionner.

2.1.2 Premiers protocoles

Comme nous venons de le voir, le théorème de non clonage et le principe d'incertitude d'Heisenberg sont des propriétés de la mécanique quantique qui peuvent avoir des conséquences intéressantes pour la cryptographie. Les premières idées de protocoles cryptographiques mettant en oeuvre ces propriétés sont apparues au début des années 80. En particulier, nous allons évoquer dans les paragraphes suivants le billet de banque quantique (*Quantum Money*) et le multiplexage quantique.

Billet de banque quantique L'idée d'utiliser les propriétés quantiques des particules pour créer des billets de banques infalsifiables a été évoquée pour la première fois au début des années 70 par Stephen Wiesner dans un manuscrit finalement publié en 1983 [Wiesner 1983].

Le principe de ce billet de banque quantique est assez simple à décrire. Au moment de la fabrication du billet de banque, un numéro de série unique habituel est associé au billet. En plus de ce numéro de série, un ensemble de n états quantiques

à 2 niveaux est incrusté dans le billet dans une mémoire quantique idéale qui maintient la cohérence du système sur de très longues périodes. Chacun de ces états est un qubit $|\phi\rangle$ qui peut se trouver dans un des quatres états $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ choisi aléatoirement. La banque conserve alors dans une base de donnée les combinaisons associées à chaque numéro de série.

Lorsque la banque se retrouve en possession d'un billet dont elle veut vérifier l'authenticité, elle peut rechercher la combinaison associée à chaque numéro de série et mesurer en fonction de celle-ci les états quantiques du billets dans la base correspondante. C'est à dire qu'elle mesure dans la base $\{|0\rangle, |1\rangle\}$ si le qubit stocké est censé avoir la valeur 0 ou 1 et inversement. Si tous les résultats de mesure correspondent aux valeurs enregistrées dans la base de donnée, la banque peut être alors certaine d'avoir à faire à un vrai billet.

Un faux-monnayeur qui souhaiterait dupliquer un vrai billet doit avant tout découvrir la combinaison cachée dans les états quantiques du billet. Or ne connaissant pas dans quelle base ils ont été choisis, il ne peut pas mesurer à tous les coups les états quantique dans la bonne base. Pour chaque qubit, il obtiendra la bonne réponse avec probabilité $3/4$. Pour $n = 15$ qubit, la probabilité qu'il ne fasse pas une seule erreur n'est plus que de 1 % environ. Il ne pourra donc pas recréer des copies identiques du billet original et la banque pourra facilement reconnaître le fraude.

La sécurité de cette méthode provient du fait qu'il est impossible de mesurer parfaitement les états quantiques dans les deux bases en même temps. En effet, les observables correspondant aux deux bases utilisées ne commutant pas, le principe d'incertitude d'Heisenberg nous assure alors qu'il est impossible d'obtenir des résultats aussi précis que souhaités dans les deux bases simultanément.

Bien sûr ce procédé est surtout un exercice théorique difficilement applicable avec la technologie actuelle. Ce protocole permet néanmoins de cerner les concepts de base de la cryptographie quantique qu'on retrouvera dans des protocoles plus aboutis de distribution quantique de clés ou d'implémentation de fonctions cryptographique sécurisées.

Multiplexage quantique Le multiplexage quantique a été étudié pour la première fois dans un article de Charles Bennett, Gilles Brassard, Seth Breidbart et Stephen Wiesner publié en 1983 [Bennett 1983].

Le principe de ce procédé est de multiplexer deux messages de façon à ce qu'il soit possible de récupérer parfaitement l'un des deux au prix de la perte définitive de l'autre. Comme pour le cas du billet de banque quantique, les messages sont encodés sur la polarisation d'un photon. Plus précisément, pour deux bits $a, b \in \{0, 1\}$ le

photon sera préparé avec un angle de polarisation égal à $(7-2a-6b+4ab)\frac{\pi}{8}$ radians.

L'encodage ainsi défini est illustré par la figure 2.1.

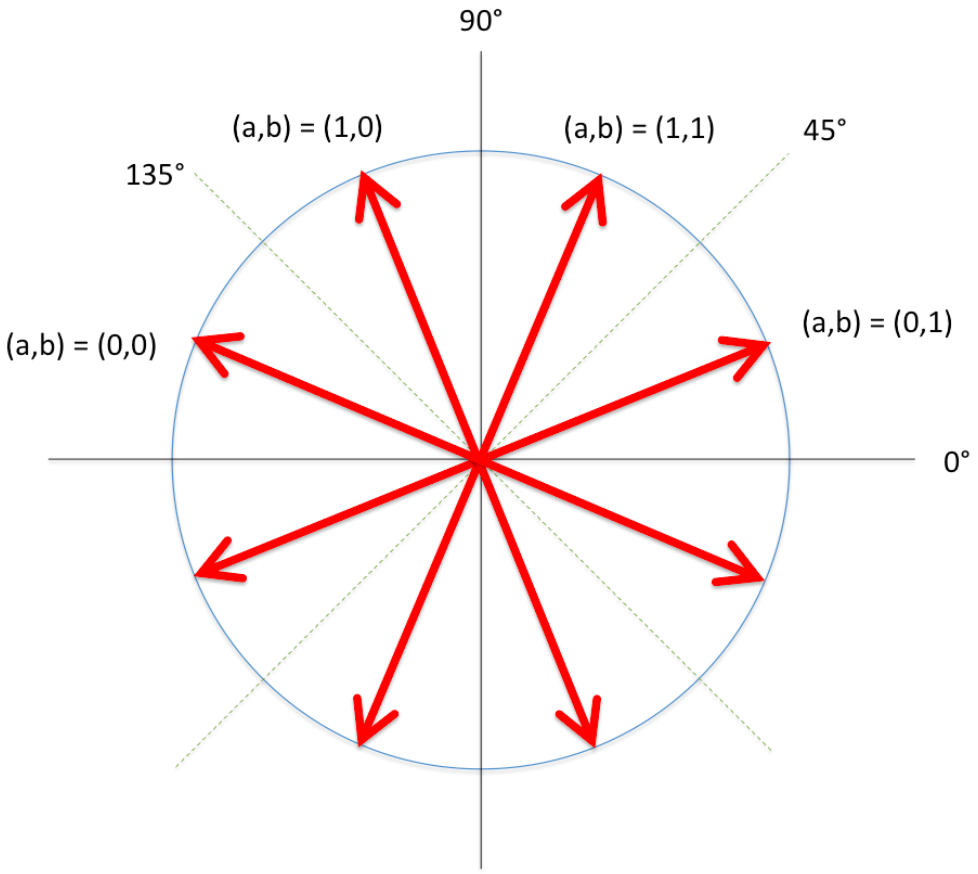


FIGURE 2.1 – Illustration de l'encodage en polarisation pour l'ensemble des couples de bits (a,b) pour le protocole de multiplexage quantique.

Les différentes valeurs possibles du couple de bits (a, b) sont représentées par un angle de polarisation de $\frac{\pi}{8}$, $\frac{3\pi}{8}$, $\frac{5\pi}{8}$ ou $\frac{7\pi}{8}$ radians.

Lorsque $a = 1$ la polarisation des photons est plus proche de la polarisation verticale quelle que soit la valeur du bit b. De même losque $a = 0$ la polarisation des photons est plus proche de la polarisation horizontale quelle que soit la valeur du bit b. Il est donc possible de déterminer la valeur du bit a avec un taux d'erreur assez faible si on mesure la polarisation des photons dans la base $(0^\circ, 90^\circ)$. Inversement il est possible de déterminer la valeur du bit b avec un taux d'erreur assez faible si on mesure la polarisation des photons dans la base $(45^\circ, 135^\circ)$.

Plus précisément, en mesurant la polarisation verticale (dans la base $(0^\circ, 90^\circ)$) du photon, le bit a est récupéré avec une probabilité d'erreur égale à $\sin^2(\frac{\pi}{8}) \approx 14,6$ %. La valeur du bit b est quant à elle obtenue avec une probabilité d'erreur de 50 %, c'est à dire que la mesure de la polarisation verticale ne donne pas d'information sur la valeur du bit b. De même en mesurant la polarisation diagonale (dans la base $(45^\circ, 135^\circ)$) du photon, le bit b peut être récupéré avec une probabilité d'erreur égale à $\sin^2(\frac{\pi}{8}) \approx 14,6$ % tandis que cette même mesure n'apporte pas d'information sur la valeur du bit a.

Si maintenant on considère des chaînes de bit a' et b' encodées à l'aide d'un code correcteur d'erreur permettant de corriger 15 % d'erreur, en mesurant dans la base $(0^\circ, 90^\circ)$ ou $(45^\circ, 135^\circ)$ Bob peut espérer récupérer parfaitement l'un ou l'autre des messages décodés a" et b". En revanche, si Bob essaie de récupérer les deux messages simultanément en utilisant une base intermédiaire entre les deux bases à utiliser pour obtenir a' ou b' il obtiendra deux chaînes de bits bruitées contenant chacune plus de 15 % d'erreur par rapport aux chaînes a' et b' et ne pourra parfaitement décoder aucune des deux chaînes.

Cette étude sommaire de la sécurité n'a pas pour objectif d'être une preuve de sécurité rigoureuse mais plutôt d'illustrer les mécanismes à l'origine de la sécurité de la plupart des protocoles de cryptographie quantique : à savoir le principe d'incertitude d'Heisenberg et le théorème de non clonage.

Les deux exemples de protocoles cryptographiques que nous venons de présenter illustrent bien les principes de base utilisés en cryptographie quantique pour justifier de la sécurité des protocoles. Cette sécurité basée sur les lois de la mécanique quantique n'est pas liée à des hypothèses de complexité algorithme ou de limitation de la puissance de calcul parfois utilisées pour justifier de la sécurité de certaines implémentations classiques de protocoles cryptographiques.

Dans la sous section suivante, nous établissons une hiérarchie entre les différents modèles de sécurité utilisés en cryptographie classique.

2.1.3 Modèles de sécurité classiques

La sécurité des primitives cryptographiques peut être évaluée dans différents modèles de sécurité plus ou moins généraux. Nous listons ici les trois principaux modèles de sécurité utilisés :

- **sécurité inconditionnelle** : ce modèle de sécurité est le plus strict. Dans ce cas, l'adversaire est supposé avoir accès à une puissance de calcul illimitée.

- **sécurité démontrable** : la sécurité d'un protocole cryptographique est démontrable lorsque l'étude peut être réduite à un problème mathématique connu qu'on suppose difficile. L'intérêt de ce modèle est de relier la sécurité d'un nouveau protocole à un problème exprimable simplement ou déjà étudié dont la difficulté est a priori mieux connue et dans laquelle on peut avoir plus confiance. Plus le problème mathématique sous-jacent a été étudié, meilleure sera la confiance dans la sécurité du protocole qui en dépend.

- **sécurité calculatoire** : la sécurité est vérifiée en estimant la difficulté de réalisation de la meilleure attaque connue sur le protocole considéré. En général il y a des similarités avec un problème mathématique connu et difficile mais contrairement au cas de la sécurité démontrable, il n'y a pas de preuve mathématique de la réduction du protocole à ce problème connu. La puissance de calcul nécessaire pour mener à bien la meilleure attaque connue sur le protocole est comparée à la puissance estimée de l'adversaire. Lorsque la différence entre les deux est jugée suffisamment importante, le protocole est considéré sûr dans le modèle de la sécurité calculatoire.

Un exemple connu de protocole de chiffrement dont il est possible de prouver la sécurité inconditionnelle est le code de Vernam ou protocole de chiffrement à masque jetable. Le chiffrement d'un message M avec une clé K à l'aide de ce protocole se fait bit à bit par l'opération logique XOR qu'on note $\oplus$. Ainsi, le message chiffré C peut s'écrire $C = M \oplus K$. L'opération de déchiffrement s'effectue de la même façon : le message déchiffré noté M' s'écrit $M' = C \oplus K = M \oplus K \oplus K = M$.

Lorsque la clé K est parfaitement aléatoire et qu'elle a une longueur au moins au grande que le message lui-même, il a été démontré [Shannon 1949] que l'entropie conditionnelle $H(M|C)$ du message clair connaissant le message chiffré était égale à $H(M)$ c'est à dire que la connaissance du chiffré ne donne pas plus d'information sur le message M que ce qui est déjà connu. De plus, un protocole de chiffrement ne peut être inconditionnellement sûr que si la longueur de la clé est au moins égale à la longueur du message. Cela signifie que tous les protocoles de chiffrement inconditionnellement sûrs sont homomorphes au protocole à masque jetable.

Un exemple de sécurité calculatoire cette fois est le protocole de cryptographie asymétrique appelé RSA. La sécurité de ce protocole est associée au problème de la factorisation des nombres entiers mais il ne s'agit pas d'un cas de sécurité démontrable puisque le protocole RSA n'est pas équivalent eu problème de la factorisation. En effet, le principe de fonctionnement de ce protocole fait qu'un adversaire capable de factoriser rapidement les nombres entiers peut facilement casser la sécurité de RSA mais le contraire n'est pas vrai. Il est possible que la difficulté du problème RSA soit bien inférieure à celle du problème de la factorisation. On dit de RSA qu'il a une sécurité calculatoire parce qu'en utilisant des clés de taille suffisante le temps

nécessaire pour casser le protocole en utilisant les meilleurs algorithmes connus peut être rendu très long. Il n'est pas contre pas exclus qu'une soudaine avancée algorithmique sur le problème RSA lui-même ou sur le problème de la factorisation rende ces estimations obsolètes.

Idéalement, on souhaiterait donc toujours utiliser des protocoles inconditionnellement sûrs. Cependant, ce niveau de sécurité absolu a un coût [2] qui rend le protocole parfois difficilement utilisable. Le meilleur exemple est la méthode de chiffrement dite du masque jetable : l'inconvénient majeur de ce protocole est que la clé doit être aussi longue que le message à envoyer. La sécurité absolue de cette méthode de chiffrement est donc obtenue au prix d'un problème de distribution de clés secrètes en quantité suffisante.

L'utilité pratique d'un protocole est donc une première raison de considérer d'autres modèles de sécurité plus souple que le modèle inconditionnel. C'est le cas pour les protocoles de chiffrement. Dans d'autres cas, comme par exemple pour certains protocoles à deux participants, il est prouvé que la sécurité inconditionnelle est tout simplement impossible à atteindre, c'est ce qui est démontré dans la sous-section suivante. On doit alors trouver un modèle de sécurité moins strict dans lequel il existe une implémentation du protocole souhaité.

2.2 Protocoles de cryptographie à deux participants

Ces protocoles font intervenir deux participants qui ne se font pas confiance. Plus précisément, ces protocoles doivent assurer un certain niveau de sécurité à un participant honnête face à un participant malhonnête qui ne respecte pas le protocole. Il faut différencier ces protocoles à deux participants des protocoles de distribution de clé par exemple dans lesquelles les deux participants se font confiance et cherchent à se protéger d'une tierce partie, l'espion.

Dans une première sous-section, nous passerons en revue plusieurs exemples importants de protocoles à deux participants en détaillant leur principe de fonctionnement. Dans une deuxième sous-section, nous étudierons les modèles de sécurité classiques utilisés et expliquerons pourquoi en particulier il n'est pas possible de créer un protocole de mise en gage de bit classique inconditionnellement sûr. Dans une dernière sous-section, nous montrerons que ce n'est pas possible non plus même en utilisant les propriétés quantiques.

2. cela peut être un coût financier, un coût en ressources de calcul ou de mémoire ou un coût en complexité d'utilisation par exemple

2.2.1 Exemples et principe de fonctionnement

Mise en gage de bit. Formalisé au début des années 80 [Even 1983], la mise en gage de bit est un protocole qui permet de fixer la valeur d'un bit tout en le gardant caché et en ayant la possibilité dans un deuxième temps de révéler la valeur de ce bit. Ce protocole peut être séparé en deux phases :

- une phase de *mise en gage* : la valeur du bit est choisie et ne peut plus être modifiée par la suite
- une phase d'*ouverture* ou de révélation : la valeur du bit est révélée

Pour formaliser la description du protocole, on appelle Alice le participant souhaitant mettre en gage le bit b auprès de Bob. La sécurité de ce protocole peut être décomposée en deux parties :

- si Alice ne peut pas modifier la valeur du bit b après la phase de mise en gage, on dit que le protocole est "engageant".
- so Bob ne peut pas obtenir d'information sur le bit b avant la phase d'ouverture, on dit que le protocole est "dissimulant".

Idéalement, un protocole de mise en gage de bit doit être à la fois parfaitement engageant et dissimulant. Nous verrons par la suite que ces deux conditions ne peuvent pas être vérifiées simultanément lorsque les participants ont accès à une puissance de calcul non bornée.

On peut néanmoins s'approcher de cette situation idéale en réalisant l'une des deux conditions. Pour illustrer notre propos, nous allons décrire un protocole parfaitement engageant pour Alice même si elle a accès à une puissance de calcul illimitée.

Exemple de protocole : Alice choisit un groupe G de générateur[3] *g et un nombre premier p tels que pour deux entiers naturels e et e' plus petits que p on a $g^e \neq g^{e'}$.*

Pour mettre en gage un entier x plus petit que p, Alice calcule $c = g^x$ et envoie à Bob le résultat. La connaissance de c ne permet pas à Bob de retrouver la valeur de x sauf s'il est capable de calculer le logarithme discret de c pour le groupe de générateur g, ce qui est un problème difficile. De son côté, Alice ne peut pas changer la valeur de l'entier x après la publication de c puisque par construction il n'existe pas d'autre entier que x qui génère c après exponentiation du générateur.

Ce protocole est donc parfaitement engageant même avec une puissance de calcul illimitée, il n'est par contre pas dissimulant contre un adversaire possédant une puissance de calcul illimitée.

3. tous les éléments du groupe peuvent être obtenus par une puissance du générateur

Transmission inconsciente La transmission inconsciente (ou *oblivious transfer* en anglais) est un protocole au cours duquel un participant envoie éventuellement un message parmi un ensemble de messages possibles sans que le destinataire puisse savoir quel message en particulier a été envoyé.

Ce protocole a été formalisé pour la première fois par Michael Rabin sous une forme appelée transmission inconsciente de Rabin [Rabin 1981]. Cette version du protocole peut être décrite de la façon suivante :

- un participant appelé Alice envoie un message m en espérant que Bob le reçoive effectivement avec probabilité $1/2$
- Alice ne peut pas savoir si le message a été reçu ou non par Bob
- Bob n'obtient pas plus de la moitié des messages

Cette première version du protocole a été généralisée par la suite avec un protocole appelée transmission inconsciente 1-2 (pour 1 message sur 2 possibles) [Even 1985].

Dans cette version, Alice choisit deux messages m_0, m_1 et Bob choisit un bit b. L'objectif de la transmission inconsciente 1-2 et de transmettre le message m_b à Bob sans qu'Alice n'apprenne la valeur du bit b et sans que Bob n'apprenne également la valeur du message $m_{\bar{b}}$.

Cette version de la transmission inconsciente avait en fait déjà été inventée par Stephen Wiesner au début des années 70 qui l'avait appelé multiplexage quantique [Wiesner 1983] comme nous l'avons vu dans une section précédente. Mais c'est seulement au début des années 80 que toutes les possibilités offertes par ce protocole ont été étudiées. En effet, il a été prouvé que la transmission inconsciente 1-2 est une primitive cryptographique universelle, c'est à dire qu'elle peut être utilisée comme brique de base pour construire n'importe quel calcul sécurisé à deux participants [Crepeau 1987] [Goldreich 1987] [Kilian 1988] . On dit dans ce cas que la transmission inconsciente 1-2 est une primitive universelle des protocoles à deux participants.

Pour finir, on peut évoquer une dernière version de la transmission inconsciente souvent utilisée dans les preuves de sécurité : la transmission inconsciente aléatoire. Dans ce cas, le résultat du protocole est de fournir à Alice deux chaînes de bits s_0, s_1 aléatoires et à Bob un bit b ainsi que la chaîne s_b associée. Comme pour le cas non aléatoire, Alice n'a pas accès au bit b et Bob n'a pas connaissance de la deuxième chaîne de bits $s_{\bar{b}}$. Cette version aléatoire est plus facile à analyser dans certains cas et une preuve de sécurité de la version aléatoire implique la sécurité de la transmission inconsciente 1-2. En effet, il est assez facile de reproduire la transmission inconsciente 1-2 à partir de la primitive de la transmission inconsciente aléatoire.

Démonstration. On suppose qu'Alice et Bob ont accès à un protocole de transmission inconsciente aléatoire : Alice obtient s_0, s_1 et Bob obtient un bit c et s_c.

Dans le protocole de la transmission inconsciente 1-2, Alice souhaite choisir les messages m_0 et m_1 à envoyer et Bob choisit le bit b correspondant au message qu'il souhaite recevoir.

1. Bob envoie dans un premier temps à Alice le résultat n du XOR (ou exclusif noté $\oplus$) du bit b et du bit c, ce faisant il ne dévoile pas d'information sur le bit b. On a $n = b \oplus c$
2. Alice envoie alors à Bob les deux messages $s_0 \oplus m_n$ et $s_1 \oplus m_{\bar{n}}$. Bob ne peut décoder qu'un seul des deux messages grâce à la chaîne de bits s_c.

On se retrouve alors dans les mêmes conditions qu'après utilisation du protocole de transmission inconsciente 1-2, ce qui conclut la preuve. □

Il existe des implémentations classiques de la transmission inconsciente [Naor 1999] [Hajiaghayi 2005] dont la sécurité est prouvée dans le cas où les adversaires ont une puissance de calcul limitée. Comme pour la mise en gage de bit, il n'existe pas de protocole classique de transmission inconsciente dont la sécurité contre un adversaire non limité est prouvée.

2.2.2 Une sécurité inconditionnelle parfois impossible à atteindre

Pour certains types de protocole, nous avons déjà vu qu'il était possible de trouver une preuve de sécurité inconditionnelle, c'est notamment le cas du chiffrement et de l'authentification [Carter 1977] [Wegman 1981]. En revanche, pour les protocoles à deux participants telles que la mise en gage de bit ou la transmission inconsciente il est impossible[4] d'obtenir une sécurité inconditionnelle [Saks 1989].

Nous présentons ici une preuve d'impossibilité pour une large classe de fonctions cryptographiques à deux participants lorsqu'un des deux est malicieux [Canetti 2006].

De manière générale, une fonction cryptographique à deux participants est caractérisée par un couple de fonctions $f = (f_1, f_2)$ correspondant aux résultats du protocoles envoyés aux participants P_1 et P_2. Chaque fonction prend comme valeur le couple (x_1, x_2) correspondant aux données apportées par les participants.

Par exemple, dans le cas de la transmission inconsciente 1-2, en reprenant les notations de la section 2.2.1 , la chaîne x_1 transmise par le participant P_1 contient l'information sur les deux messages $m_0, m1$ et la chaîne x_2 transmise par le participant P_2 contient l'information sur le bit b. En retour, $f_1(x_1, x_2)$ contient une

4. On peut en revanche noter qu'il est possible d'obtenir une preuve de sécurité inconditionnelle si on accepte de ne pas réaliser parfaitement la primitive [Aharonov 2000, Chailloux 2009]

confirmation de la bonne transmission d'un des deux messages et $f_2(x_1, x_2)$ *contient le message* m_b.

La preuve d'impossibilité se base sur une propriété non désirée de la fonction f : cette fonction est dite **complètement révélatrice** pour un des participants, par exemple P_1, si l'autre participant peut obtenir des informations sur x_1 en choisissant judicieusement sa chaîne x_2. Plus formellement, une fonction $f = (f_1, f_2)$ est dite complètement révélatrice pour P_1 si il existe une chaîne d'entrée x_2 telle que la fonction $f_2(x_1, x_2)$ permette de retrouver x_1 quelle que soit sa valeur.

Le théorème 4.7 de [Canetti 2006] nous assure qu'il n'existe pas de fonction cryptographique à deux participant inconditionnellement sûre qui ne soit pas également complètement révélatrice.

Théorème : Soit $f = (f_1, f_2)$ une fonction à deux participants qui n'est pas complètement révélatrice. Soit $\mathcal{F}_f$ la fonction idéale qui reçoit x_1 et x_2 en entrée de la part des participants P_1 et P_2 et renvoie $f_1(x_1, x_2)$ et $f_2(x_1, x_2)$ à P_1 et P_2 respectivement. Alors $\mathcal{F}_f$ ne peut pas être réalisée de manière sécurisée.

Ce résultat nous permet alors de facilement prouver l'impossibilité d'obtenir un protocole inconditionnellement sûr réalisant la transmission inconsciente 1-2. En effet, par construction le transfert inconscient 1-2 ne peut pas être complètement révélateur pour aucun des deux participants. Il existe également des preuves d'impossibilité concernant la fonction de mise en gage de bit [Datta 2006][Canetti 2001].

Après l'obtention de ces résultats d'impossibilité pour des fonctions cryptographiques, l'attention s'est portée sur la possibilité d'utiliser les propriétés quantiques pour obtenir des protocoles à deux participants inconditionnellement sûrs. Comme nous l'étudions dans la sous-section suivante, cette recherche s'est finalement révélée être infructueuse.

2.2.3 La mise en gage quantique inconditionnellement sûre est impossible

Premières tentatives d'implémentation en quantique

Les premières tentatives de création de protocoles cryptographiques à deux participants sont apparues dès le début de l'information quantique avec notamment le tirage à pile ou face quantique proposé dans le même article que le premier protocole de distribution quantique de clés [Bennett 1984]. Ce protocole peut en fait être facilement adapté pour se transformer en une mise en gage de bit quantique. Mais déjà cet article évoque la possibilité de triche basée sur l'utilisation de l'intrication.

Plus tard, de nombreux autres protocoles quantiques de cryptographie à deux participants ont été proposés [Crépeau 1988][Brassard 1991][Brassard 1993] et la sé-

curité inconditionnelle des ces protocoles paraissaient avoir été prouvées. Mais il a été découvert [Mayers 1996a] que ces protocoles étaient en fait vulnérables au même type d'attaque que celles déjà évoquées dans [Bennett 1984].

La mise en gage de bit quantique est impossible

Finalement, l'impossibilité de la mise en gage de bit quantique a été prouvée définitivement par Dominic Mayers [Mayers 1996b] et Hoi Kwong Lo [Lo 1997]. Nous ne détaillerons pas ici la preuve du théorème d'impossibilité [Mayers 1996b] mais pour mieux comprendre le mécanisme permettant à un participant malhonnête de faire échouer un protocole de mise en gage quantique nous allons expliciter l'attaque élaborée dans [Mayers 1996a] contre le protocole introduit dans [Brassard 1993].

En effet, cette attaque s'explique facilement en s'appuyant sur un théorème sur la classification des systèmes quantiques [Hughston 1993] :

Théorème : Soient $\psi_1, \psi_2, \ldots, \psi_n$ et $\varphi_1, \varphi_2, \ldots, \varphi_n$ deux ensembles d'états quantiques associés à des distributions de probabilité et décrits par la même matrice densité ρ. Alors il est possible de construire un système bipartite $A \otimes B$ de matrice densité ρ_{AB} tel que $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ est égal à la matrice densité ρ et tel qu'il existe un couple d'opérateurs de mesure M_ψ, M_φ qui vérifie la propriété suivante : l'application de la mesure M_ψ au système A donne le résultat i de l'indice de l'état ψ_i sur lequel est projeté le système B (de même l'application de la mesure M_φ au système A donne le résultat i de l'indice de l'état φ_i sur lequel est projeté le système B).

Moins formellement, cela signifie que dans un protocole de mise en gage quantique où Alice transmet à Bob un état quantique contenant la valeur du bit qu'elle met en gage, Alice peut toujours conserver dans son laboratoire un système quantique intriqué avec celui de Bob et choisir a posteriori le bit mis en gage. C'est le principe de l'attaque exposée dans [Mayers 1996a] sur une proposition de protocole de mise en gage quantique de bit basée sur les états BB84 [Brassard 1993].

De plus, nous avons déjà évoqué que la transmission inconsciente 1-2 est une primitive cryptographique universelle des fonctions cryptographiques à deux participants (en particulier il est possible de construire un protocole de mise en gage de bit à partir de cette primitive). La preuve d'impossibilité sur la mise en gage de bit quantique implique donc l'impossibilité de créer un protocole de transmission inconsciente inconditionnellement sûr.

Recherche d'autres modèles de sécurité

Ces preuves d'impossibilité pour des adversaires non limités ont favorisé la recherche de modèles de sécurité où la puissance de l'adversaire est limitée. Ainsi, la sécurité

d'un protocole de transmission inconsciente a été prouvée dans le cas où l'adversaire ne peut pas stocker de photon sur de longues périodes et est limité à des mesures de Von Neumann [Crépeau 1994]. La sécurité de ce même protocole a même été prouvée dans le cas où l'adversaire peut effectuer des mesures générales mais sur un seul photon à la fois [Mayers 1994].

Enfin, des modèles plus généraux dans lesquels la sécurité des fonctions cryptographiques à deux participants peut être prouvée ont été développés : le modèle de la mémoire bornée dans lequel l'adversaire a accès à une quantité limitée de mémoire quantique et le modèle de la mémoire bruitée dans lequel l'adversaire a accès à une mémoire bruitée. Ces modèles sont étudiés plus en détail dans la section suivante.

2.3 Nouveaux modèles de sécurité en cryptographie quantique

Nous présentons dans cette section des nouveaux modèles de sécurité où la puissance de l'adversaire est limitée et dans lesquels il est possible d'obtenir des résultats sur la sécurité des fonctions cryptographiques à deux participants. Nous présentons brièvement le modèle de la mémoire quantique bornée dans une première sous-section avant de nous attarder plus longuement sur le modèle plus général de la mémoire bruitée (qui inclus le modèle de la mémoire bornée).

2.3.1 Modèle de la mémoire (quantique) bornée

Ce modèle de sécurité a d'abord été étudié dans un contexte classique. Dans ce cas, le modèle suppose que l'adversaire a accès à une capacité de calcul illimitée mais une quantité de mémoire classique bornée, la borne pouvant prendre la forme d'une quantité absolue de mémoire ou d'un taux de stockage maximum par exemple. Dans ce modèle de sécurité, il est possible de prouver la sécurité d'un système de distribution de clé [Maurer 1992] ou d'un protocole de transmission inconsciente 1-2 [Cachin 1998].

Cependant, étant donné la disponibilité, le coût et la qualité de la mémoire classique accessible à un adversaire, il faudrait que la quantité de mémoire limite de l'adversaire soit exponentiellement plus élevée que la mémoire nécessaire aux participants honnêtes pour que le modèle de sécurité de la mémoire classique bornée soit intéressant. Or cette borne est au mieux quadratique par rapport à la quantité de mémoire nécessaire aux participants honnêtes [Ding 2007]. Ainsi, ce modèle ne permet pas de créer une dissymétrie suffisamment importante entre les ressources nécessaires à un adversaire pour casser la sécurité par rapport aux ressources nécessaires aux participants honnêtes.

L'idée du modèle de la mémoire quantique bornée est d'imposer une limite sur la

quantité de mémoire quantique tout en laissant une quantité non bornée de mémoire classique à l'adversaire. Ces restrictions sont beaucoup plus raisonnables puisqu'il y a une grande différence entre la quantité de mémoire quantique nécessaire aux participants honnêtes et la quantité nécessaire à un adversaire : en effet il est possible d'obtenir des protocoles qui ne nécessitent pas l'utilisation de mémoire quantique par les participants honnêtes alors qu'un adversaire a besoin de mémoire quantique pour tricher. Cette dissymétrie entre participants honnêtes et adversaires associé à la grande difficulté technologique de fabrication de mémoire quantique rend ce modèle plus séduisant que le modèle de sécurité de la mémoire classique bornée.

Résultats obtenus dans ce modèle

Lorsque la mémoire quantique de l'adversaire est bornée, il est possible d'implémenter un protocole de mise en gage quantique et un protocole de transmission inconsciente [Damgaard 2005]. Plus précisément, la preuve de sécurité pour le protocole de transmission inconsciente est valable lorsque la mémoire de l'adversaire est inférieure au quart du nombre de qubits échangés au cours du protocole. En terme de taux de stockage, cette borne signifie que le protocole est sûr lorsque l'adversaire ne peut stocker plus du quart des qubits échangés. De leur côté, les participants honnêtes n'ont pas besoin de mémoire quantique pour mettre en oeuvre le protocole qui peut donc être implémenté avec la technologie existante en laboratoire.

Les limites du modèle de la mémoire quantique bornée

Une façon plus proche de la réalité de limiter la puissance de l'espion serait de considérer le niveau de bruit de sa mémoire quantique. En effet, un adversaire a plus probablement accès à une mémoire quantique bruitée qu'une mémoire quantique parfaite. Il pourrait donc être intéressant de généraliser le modèle de la mémoire quantique bornée au cas où cette mémoire peut être bruitée.

Comme nous allons le voir dans la sous-section suivante, il se trouve que le modèle de la mémoire quantique bruitée permet effectivement d'obtenir des bornes de sécurité intéressantes pour des protocoles implémentant des fonctions cryptographiques à deux participants.

2.3.2 Modèle de la mémoire (quantique) bruitée

Ce modèle de sécurité est une version généralisée du modèle de la mémoire quantique bornée. Dans ce modèle, on considère que l'adversaire a accès à une quantité finie [5] de mémoire quantique bruitée [Wehner 2008] [Koenig 2009b]. Ainsi, le modèle

5. La restriction de l'adversaire à une quantité finie de mémoire quantique bruitée est nécessaire : en effet, un adversaire en possession d'un ordinateur quantique arbitrairement puissant pourrait

présenté dans la sous-section précédente est un cas particulier du modèle de la mémoire quantique bruitée.

Nous allons commencer par détailler le formalisme mathématique du modèle de la mémoire bruitée avant d'exposer les principaux résultats obtenus grâce à ce modèle.

Description mathématique de la mémoire quantique de l'adversaire
Dans ce modèle, l'adversaire a accès à une mémoire quantique bruitée dont il faut préciser la définition mathématique. Une mémoire quantique est un dispositif qui permet de stocker des états quantiques décrits dans un espace de Hilbert noté $\mathcal{H}_{\text{in}}$. L'évolution d'un état quantique $\rho \in \mathcal{H}_{\text{in}}$ stocké dans la mémoire est caractérisée par un opérateur positif conservant la trace que l'on note

$$\mathcal{F}_t \ : \ \mathcal{S}(\mathcal{H}_{\text{in}}) \longrightarrow \mathcal{S}(\mathcal{H}_{\text{out}}). \tag{2.14}$$

L'ensemble des temps de stockage $t \geq 0$ définit une famille d'opérateurs $\{\mathcal{F}_t\}_{t\geq 0}$ dont on peut raisonnablement supposer qu'ils vérifient les propriétés suivantes :

- $\mathcal{F}_0 = \text{Id}$: c'est à dire qu'un temps de stockage nul est équivalent à une absence de bruit,
- $\mathcal{F}_{t_1+t_2} = \mathcal{F}_{t_1} \circ \mathcal{F}_{t_2}$: le bruit augmente avec le temps passé dans la mémoire.

Ainsi, l'adversaire n'a aucun intérêt à laisser un état quantique plus longtemps que nécessaire dans la mémoire quantique. Si un protocole impose un délai d'attente Δt, on peut alors considérer que la mémoire quantique de l'adversaire est décrite par l'opérateur $\mathcal{F} = \mathcal{F}_{\Delta t}$.

Pour obtenir des résultats numériques, il est nécessaire de préciser la structure de cet opérateur. On considère alors souvent qu'il est un produit tensoriel de canaux bruités agissant sur des qubits. On peut faire cette hypothèse sans perte de généralité puisque cela ne diminue pas la puissance de l'adversaire, une mémoire ayant cette structure étant capable de stocker n'importe quel état quantique pourvu qu'il ait accès à une ordinateur quantique, ce qui est le cas. Par exemple, pour un nombre n de qubits échangés par les participants au cours du protocole, l'opérateur décrivant la mémoire de l'adversaire s'écrit

$$\mathcal{F} = \mathcal{N}^{\otimes \nu n} \tag{2.15}$$

où $\mathcal{N} \ : \ \mathcal{S}(\mathbb{C}^2) \longrightarrow \mathcal{S}(\mathbb{C}^2)$ est un canal bruité agissant sur des qubits et ν représente le taux de stockage de l'adversaire.

toujours utiliser des codes correcteurs d'erreur quantiques pour transformer une quantité infinie de mémoire quantique bruitée en une quantité infinie de mémoire quantique parfaite.

Le choix du canal $\mathcal{N}$ dépend du type de mémoire considéré. Dans la littérature, c'est souvent le canal à dépolarisation qui est utilisé. La définition mathématique de ce canal se trouve à la page 21.

Contraintes imposées à l'adversaire

Un protocole dont on veut prouver la sécurité dans le modèle de la mémoire bruitée doit introduire un temps d'attente minimum Δt pendant lequel un adversaire malicieux doit stocker tous les états quantiques qu'il souhaite conserver dans une mémoire quantique décrite par un opérateur $\mathcal{F}$. Les contraintes imposées à l'adversaire sont :

- l'adversaire a une capacité de stockage classique et des ressources de calcul quantique illimitées,
- les actions de communication, calcul, préparation et mesure d'états quantiques sont instantanées et sans bruit,
- lorsque le protocole introduit un temps d'attente Δt, l'adversaire peut stocker une partie du système quantique en sa possession en l'encodant dans l'espace de Hilbert $\mathcal{H}_{\text{in}}$ et doit mesurer immédiatement tout ce qui n'a pas été stocké dans la mémoire quantique bruitée.

Tout l'intérêt de ce modèle est de mesurer la perte d'information provoquée par la troisième contrainte imposée à l'adversaire. Pour évaluer cette perte d'information, la bonne grandeur à considérer est la probabilité de correctement décoder l'information transmise à travers le canal $\mathcal{F}$ représentant la mémoire quantique. Cette probabilité est définie par la relation

$$\forall n \in \mathbb{N}, \qquad P_{\text{succ}}^{\mathcal{F}}(n) = \max_{\{D_x\}_x, \{\rho_x\}_x} \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Tr}\left(D_x \mathcal{F}(\rho_x)\right) \tag{2.16}$$

où la maximisation est faite sur l'ensemble des familles de codes $\{\rho_x\}_{x\in\{0,1\}^n}$ sur l'espace de Hilbert $\mathcal{H}_{\text{in}}$ et l'ensemble des POVMs de décodage $\{D_x\}_{x\in\{0,1\}^n}$ sur $\mathcal{H}_{\text{out}}$.

Un des résultats majeurs de [Wehner 2008] est de prouver la sécurité des protocoles implémentant des fonctions cryptographiques à deux participants dans le modèle de la mémoire bruitée lorsque cette probabilité de décodage $P_{\text{succ}}^{\mathcal{F}}(n)$ décroît exponentiellement lorsque n tend vers l'infini.

Cette décroissance exponentielle est en générale difficile à prouver mais si le canal $\mathcal{F}$ peut s'écrire sous la forme d'un produit tensoriel $\mathcal{N}^{\otimes n}$ de canaux à dépolarisation alos la propriété suivante est vérifiée [Koenig 2009a] :

Pour un taux $R = \frac{m}{n}$ supérieur à la capacité classique du canal $C_{\mathcal{N}}$ on a

$$\exists\ \gamma^{\mathcal{N}}(R) > 0 \quad \textit{tel que} \quad P_{succ}^{\mathcal{N}^{\otimes n}}(m) \leq 2^{-n\gamma^{\mathcal{N}}(R)}. \tag{2.17}$$

La probabilité de succès décroît ainsi exponentiellement vers 0 lorsque le taux R est supérieur à la capacité classique du canal $C_{\mathcal{N}}$.

Lorsque la probabilité de succès du décodage est suffisamment faible, cela permet de borner la capacité de l'adversaire à transmettre de l'information utile à travers sa mémoire quantique bruitée. Mathématiquement, si l'adversaire est en possession d'un état quantique Q contenant de l'information sur la variable aléatoire X alors le stockage de l'état quantique dans la mémoire se traduit par une perte d'information. En terme de min-entropie cela signifie que

$$H_{\min}(X|\mathcal{F}(Q)) \geq H_{\min}(X|Q) \tag{2.18}$$

qui traduit le fait que l'adversaire ne peut pas gagner d'information en plaçant son état quantique dans une mémoire bruitée.

En général cette inégalité n'est pas suffisante pour les preuves de sécurité. Il est nécessaire de quantifier plus précisément l'augmentation de la min-entropie par l'action du bruit dans la mémoire. Cette augmentation est caractérisée par le lemme 2.1 de l'article [Koenig 2009a] :

Pour un état classique-quantique arbitraire ρ_{XQ} et un canal bruité $\mathcal{F} : \mathcal{S}(\mathcal{H}_Q) \longrightarrow \mathcal{S}(\mathcal{H}_{out})$, on a

$$H_{\min}(X|\mathcal{F}(Q)) \geq -\log P_{\text{succ}}^{\mathcal{F}}(\lfloor H_{\min}(X)\rfloor). \tag{2.19}$$

C'est cette relation (ou une version similaire concernant la min-entropie lissée) qui est utilisée dans les preuves de sécurité dans le modèle de la mémoire bruitée.

Dans le chapitre 5, nous utilisons une relation de ce type pour calculer le taux de clé secrète de différents protocoles de distribution quantique de clés dans le modèle de la mémoire bruitée.

Preuves de sécurité dans ce modèle

Dans [Koenig 2009a], la sécurité d'un protocole de mise en gage quantique de bit et d'un protocole de transmission inconsciente 1-2 est établie dans le modèle de la mémoire bruitée grâce à la méthode évoquée précédemment [6].

6. En fait, les protocoles de mise en gage quantique et de transmission inconsciente 1-2 sont fabriqués à partir d'une primitive appelée *Weak String Erasure* dont la sécurité est établie dans le modèle de la mémoire bruitée.

Ainsi, pour un canal représentant la mémoire de l'espion de la forme $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$, en notant $C_{\mathcal{N}}$ la capacité classique du canal $\mathcal{N}$, les protocoles de mise en gage quantique et de transmission inconsciente sont sûrs à condition que

$$C_{\mathcal{N}}.\nu < \frac{1}{2}. \tag{2.20}$$

Ce résultat améliore la borne obtenue dans le cadre du modèle de la mémoire bornée puisque dans le cas d'une mémoire parfaite ($C_{\mathcal{N}} = 1$) on obtient la condition $\nu < \frac{1}{2}$. On rappelle que le résultat précédent ne garantissait la sécurité de ces protocoles que pour $\nu < \frac{1}{4}$ [Damgaard 2007].

2.3.3 Adaptation du modèle de la mémoire bruitée à la distribution quantique de clés

Le modèle de la mémoire bruitée tel que présenté ici a été développé pour l'analyse de la sécurité de protocoles de cryptographie impliquant deux participants dont l'un des deux est malhonnête. Dans ce cas l'adversaire est un des participants.

Dans le cas de la distribution quantique de clés, deux participants honnêtes collaborent pour créer une chaîne commune de bits secret en empêchant l'adversaire (ou l'espion) d'obtenir de l'information sur cette chaîne de bits. Il faut donc adapter le modèle de sécurité à cette situation où deux participants collaborent face à un adversaire.

Ce travail d'adaptation du modèle de sécurité ainsi que les preuves de sécurité qui en découlent sont présentés dans le chapitre 5.

Chapitre 3

Sécurité des systèmes de distribution quantique de clés

Sommaire

La distribution quantique de clés est une méthode permettant de produire une clé secrète partagée par deux utilisateurs distants. L'avantage des protocoles de distribution quantique de clés est qu'il est possible de prouver la sécurité inconditionnelle des clés produites. Cela a en effet été démontré pour BB84 [Shor 2000] et d'autres protocoles de distribution quantique de clés par la suite [Renner 2005a]

[Cirac 2009]. Dans ces conditions, il est possible de calculer des taux de clés secrètes atteignables contre un adversaire limité par les seules lois de la mécanique quantique.

L'objectif de cette thèse est d'étudier le compromis entre la sécurité du protocole et le gain de performance [1] obtenu lorsque l'on passe de ce modèle le plus général à un modèle de sécurité plus restrictif où l'adversaire n'a plus accès à une mémoire quantique parfaite.

Pour quantifier précisément cette amélioration de performance, il est nécessaire de bien comprendre les modèles de sécurité standards utilisés dans l'étude de la sécurité des systèmes de distribution quantique de clés. Après avoir rappelé le principe général de la distribution quantique de clés, nous présenterons le principe de fonctionnement des protocoles dont la sécurité est étudiée dans les chapitres suivants. Ensuite, à partir de l'analyse des modèles de sécurité utilisés jusqu'à présent, nous expliquerons pourquoi il nous paraît pertinent aujourd'hui d'introduire de nouveaux modèles de sécurité dans lesquels la qualité ou la quantité de la mémoire quantique sont limitées.

3.1 Principe général de la distribution quantique de clés

3.1.1 Objectif du protocole

La distribution quantique de clés est un protocole permettant de réaliser une primitive cryptographique très importante : l'établissement d'un secret commun entre deux utilisateurs distants ayant à leur disposition des canaux publics dont on précisera la nature un peu plus loin. Les clés produites par ce protocole peuvent ensuite être utilisée par un protocole de chiffrement (le code de Vernam par exemple [2]) pour établir un canal privé entre les deux participants.

Généralement, on appelle Alice et Bob les deux utilisateurs souhaitant établir une clé secrète commune. L'objectif du protocole est de s'assurer que l'adversaire ou espion appelé Eve ne puisse pas obtenir d'information sur la clé partagée par Alice et Bob. Comme nous le verrons dans la suite de ce chapitre, la distribution quantique de clés permet d'atteindre cet objectif avec l'assurance d'une sécurité inconditionnelle, c'est à dire où on ne fait aucune supposition sur la puissance de l'espion.

3.1.2 Ressources nécessaires aux protocoles de distribution quantique de clés

Tous les protocoles de distribution quantique de clés nécessitent au moins un canal quantique public (l'espion peut accéder à ce canal et le manipuler) et un canal

1. que ce gain soit en terme de débit de clé ou de distance accessible
2. appelé également code à masque jetable ou *one-time pad*

classique authentifié (l'espion a accès à son contenu mais ne peut pas modifier les messages qui y passent). L'accès à un canal authentifié est absolument nécessaire pour se prémunir contre une attaque de type *man in the middle*[3].

Cette condition d'accès à un canal classique authentique n'est pas aussi forte qu'on pourrait le croire a priori pour deux raisons :

- il est possible de créer un canal authentifié à partir d'un canal non sécurisé et d'un secret pré-partagé relativement court grâce à des protocoles d'authentification inconditionnellement sûrs [Carter 1977] [Wegman 1981],

- l'accès à un canal classique authentifié ne permet pas à lui seul à Alice et Bob de générer un secret commun [Maurer 1993], cette contrainte est donc moins forte que l'objectif de création d'un canal privé .

Finalement, les ressources nécessaires à la réalisation d'un protocole de distribution quantique de clés peuvent être réduites à l'accès à un canal quantique et au partage préalable d'une petite quantité de secret.

3.1.3 Origine de la sécurité

Comme nous l'avons déjà évoqué dans le premier chapitre, l'idée de la distribution quantique de clés provient de l'impossibilité d'observer un système quantique sans le perturber. Un espion qui tenterait d'intercepter les états quantiques envoyés par Alice et Bob introduirait forcément des erreurs qui seraient alors repérées par les participants.

Ainsi, un espion passif qui ne ferait qu'observer le trafic quantique et classique ne pourrait pas obtenir d'information sur la clé et Alice et Bob pourraient alors parvenir à amplifier leur secret pré-partagé autant qu'ils le souhaitent. Si Alice et Bob repèrent la présence d'un espion actif ils peuvent simplement décider de ne pas utiliser les clés générées : si les actions de l'espion conduisent au tarissement de la source de secret pré-partagé entre Alice et Bob, la seule conséquence de ses actions serait un déni de service et pas une compromission de la sécurité.

Pour quantifier la relation entre perturbation causée par l'espion et fuite d'information, il faut détailler le fonctionnement des protocoles utilisés. Dans la section suivante, nous présentons le principe de fonctionnement des trois protocoles de distribution quantique de clés qui seront ensuite considérés dans cette thèse.

3. Attaque de l'homme du milieu : l'attaquant se fait passer pour Bob auprès d'Alice et pour Alice auprès de Bob. Cette attaque est notamment possible lorsque Alice et Bob n'ont aucun moyen de s'identifier

3.2 Présentation des protocoles étudiés

Les protocoles de distribution quantique de clés présentés ici suivent à peu près la même structure. Nous détaillons donc le déroulement de ces protocoles en s'appuyant sur l'exemple de BB84 dans la première sous-section avant de présenter de manière plus concise le principe de fonctionnement de deux autres protocoles de distribution quantique de clés dans les sous-sections suivantes.

3.2.1 BB84

Ce protocole de distribution quantique de clés utilise comme vecteur de l'information la polarisation des photons, un système quantique à deux niveaux [Bennett 1984]. L'état de polarisation du photon peut être décrit dans deux bases orthogonales appelées base rectiligne et base diagonale. Ces deux bases sont mutuellement non biaisées c'est à dire qu'une mesure effectuée dans une de ces bases n'apporte pas d'information sur le résultat de la mesure du même état dans l'autre base.

Pour BB84, on note ces bases $\{|0\rangle, |1\rangle\}$ et $\{|+\rangle, |-\rangle\}$ pour la base rectiligne et la base diagonale respectivement. Cela signifie que l'état correspondant au bit classique $x \in \{0, 1\}$ dans la base $b \in \{0, 1\}$ s'écrit $H^b |x\rangle$ où H est la transformation de Hadamard.

Pour décrire le principe de fonctionnement de ce protocole, nous pouvons distinguer cinq étapes principales : la communication quantique, le tamisage, l'estimation de paramètre, la correction d'erreur et l'amplification de confidentialité.

1. **communication quantique** : lors de cette première étape, Alice choisit aléatoirement n bits représentés par la variable aléatoire $X = (X_1, \ldots, X_n)$ et encode ces bits aléatoirement dans l'une des deux bases de polarisation. Alice prépare donc l'état $H^{b_1} |x_1\rangle \otimes \cdots \otimes H^{b_n} |x_n\rangle$ et le transmet à Bob par l'intermédiaire du canal quantique. Ce dernier mesure ces qubits dans une base choisie aléatoirement : on note $Y = (Y_1, \ldots, Y_n)$ la variable aléatoire représentant le résultat de ses mesures.

2. **phase de tamisage** : Alice et Bob annoncent publiquement leur choix de base. Ils choisissent alors de ne conserver que les bits pour lesquels leur choix de base coïncide. En moyenne ces chaînes sont donc deux fois plus courtes que les chaînes de départ X et Y.

3. **estimation de paramètre** : Alice et Bob dévoilent publiquement une petite partie (choisie aléatoirement) de leurs résultats de mesure pour estimer le taux d'erreur entre leurs chaînes de bits respectives. Si ce taux d'erreur est trop élevé, ils peuvent choisir d'interrompre le protocole ici. En effet, un taux d'erreur trop élevé peut être le signe de la présence d'un espion sur le canal

quantique. On note X' et Y' les chaînes de bits restants à ce stade du protocole.

4. **correction d'erreur** : en fonction du taux d'erreur estimé lors de la phase précédente, Alice envoie à Bob l'information lui permettant de reconstruire X' à partir de sa chaîne Y'. Alice et Bob sont alors en possession de la même chaîne de bits sur laquelle l'espion peut avoir de l'information.

5. **amplification de confidentialité** : Alice et Bob utilisent une technique de hachage universel pour obtenir une clé secrète à partir de leurs chaînes de bits partiellement secrètes.

Une analyse rapide permet de comprendre pourquoi ce protocole permet de garantir la confidentialité de la clé générée.

Le premier scénario imaginable est qu'un espion décide de mesurer certains des qubits envoyés par Alice. Dans ce cas, Bob peut utiliser le canal classique authentifié pour prévenir Alice de la non réception des ces qubits. Les bits identifiés peuvent donc être éliminés avant de poursuivre normalement le protocole. La seule conséquence de cette attaque est un possible déni de service si l'espion intercepte tous les qubits.

Afin d'éviter de dévoiler sa présence en interceptant des qubits, un espion pourrait alors tenter de cloner les qubits au cours de la transmission d'Alice à Bob. Mais comme nous l'avons déjà expliqué dans le chapitre précédent, il n'est pas possible de cloner parfaitement un état quantique inconnu. Ce faisant, l'action de l'espion se traduirait forcément par des erreurs dans les mesures de Bob. Les participants honnêtes pourraient alors se rendre compte de la tentative d'espionnage au cours de la phase d'estimation de paramètre et décider d'interrompre le protocole. Ici encore la seule conséquence de cette attaque peut être une diminution du taux de clé secrète ou un déni de service au pire mais ne compromet pas la sécurité du protocole.

3.2.2 *Six-states*

Le protocole de distribution quantique de clés appelé communément *six-states* (protocoles à 6 états) est une généralisation de BB84 dans laquelle une troisième base d'encodage de la polarisation est ajoutée [Bruß 1998].

Ainsi, Alice peut choisir d'encoder ses bits dans une des deux bases de BB84, $\{|0\rangle, |1\rangle\}$ et $\{|+\rangle, |-\rangle\}$, ou dans une troisième base notée $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$ qui correspond à l'état de polarisation circulaire gauche et droite avec $|\circlearrowleft\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$ et $|\circlearrowright\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$.

L'ajout de cette troisième base rend l'étude de la sécurité de ce protocole plus simple que pour BB84 en symétrisant le problème : en mesurant les paramètres du

canal sur 3 bases au lieu de 2 les participants honnêtes ont une meilleure connaissance du canal ce qui limite les possibilités d'action de l'espion et donc le nombre de paramètres nécessaires à la description de l'attaque. De plus, il n'est pas nécessaire d'utiliser plus de 3 bases différentes pour connaître parfaitement le canal dans le cas de BB84. En effet, il est connu que pour un espace de Hilbert de dimension d avec d une puissance entière d'un nombre premier, le nombre de bases mutuellement non biaisées est égal à $d+1$ [Durt 2010]. Dans le cas de qubits il y a donc bien 3 bases mutuellement non biaisées possibles.

L'autre avantage de ce protocole est de compliquer la tâche de l'espion : si celui-ci intercepte l'ensemble des qubits et renvoie à Bob sa meilleure estimation le taux d'erreur enregistré par Bob sera de 33 % au lieu de 25 % dans le cas de BB84. En augmentant le nombre de bases, la probabilité que l'espion mesure le qubits dans la bonne base est diminuée. On verra dans la suite de ce chapitre que cet avantage par rapport à BB84 se retrouve dans des modèles de sécurité plus généraux.

L'inconvénient majeur de ce protocole est qu'Alice et Bob mesurent dans la même base seulement $1/3$ du temps au lieu de la moitié du temps pour BB84. Toute chose étant égale par ailleurs, le taux de clé sera donc moins élevé.

Enfin, un dernier inconvénient technologique est que l'implémentation de ce protocole nécessite des dispositifs supplémentaires qui produisent des pertes supplémentaires par rapport à un dispositif équivalent implémentant BB84 [Gisin 2002].

Comme nous le verrons pas la suite, l'étude de la sécurité du protocole *six-states* peut en général se déduire de l'étude de la sécurité de BB84. Le fait qu'Alice et Bob puissent utiliser une troisième base améliore leur connaissance du canal et ajoute une contrainte supplémentaire sur les actions possibles de l'espion sur le canal quantique. Cela a pour effet de réduire le nombre de degrés de liberté de l'attaque de l'espion et simplifie donc l'optimisation.

3.2.3 SARG04

Le protocole de distribution quantique de clés SARG04 est une version modifiée [Scarani 2004] de BB84 dans lequel la phase de communication quantique est inchangée et où seule la phase de réconciliation classique est modifiée.

Ainsi, SARG04 utilise les mêmes états quantiques que le protocole BB84 avec un encodage différent des bits secrets. Tout comme dans BB84, Alice prépare un état $H^b |x\rangle$ dans lequel le bit secret est cette fois représenté par le choix de la base b plutôt que par x. De cette façon, les états $|0\rangle$ et $|1\rangle$ représentent le bit secret "0" et les états $|+\rangle$ et $|-\rangle$ représentent le bit secret "1".

Pour expliquer le principe de la phase de réconciliation, nous détaillons un

exemple d'échange : on considère qu'Alice choisit le bit secret "0" et qu'elle l'encode avec l'état $|0\rangle$ sélectionné aléatoirement parmi l'ensemble $\{|0\rangle, |1\rangle\}$. Le bit sera conservé par Alice et Bob si ce dernier a choisi de mesurer le qubit dans la base $\{|+\rangle, |-\rangle\}$ (ce qui arrive une fois sur deux). Dans ce cas Bob peut obtenir un des 2 résultats de mesure "+" ou "-" de manière équiprobable.

Pendant la phase de réconciliation, Alice va annoncer que l'état quantique envoyé faisait partie de l'ensemble $\{|0\rangle, |+\rangle\}$. Cela permet à Bob d'identifier l'état réellement envoyé comme étant $|0\rangle$ si il a obtenu le résultat "-". De même si Alice annonce que l'état quantique envoyé faisait partie de l'ensemble $\{|0\rangle, |-\rangle\}$ alors Bob peut identifier l'état réellement envoyé comme étant $|0\rangle$ s'il a obtenu le résultat "+".

L'inconvénient de ce protocole est que la chaîne de bits obtenue après la phase de tamisage est 4 fois plus courte que la chaîne de bits envoyée par Alice (contrairement à BB84 où le rapport est seulement de 1/2). En effet, Bob a une chance sur 2 de mesurer dans la bonne base et encore une chance sur 2 d'obtenir le bon résultat.

Ce protocole a par contre plusieurs avantages :

- en conservant la même phase de communication quantique que BB84, ce protocole est directement implémentable sur un dispositif optique réalisant BB84 sans changement de matériel.

- alors que certaines implémentations de BB84 à base de laser atténué sont très sensibles aux attaques par "partage du nombre de photons" appelées attaques PNS [Brassard 2000][Lütkenhaus 2000], le protocole SARG04 résiste beaucoup mieux [Branciard 2005].

Ce dernier avantage a finalement quelque peu perdu de son intérêt lorsqu'en 2003 une nouvelle méthode permettant de se protéger des attaques PNS a été inventée. Ce nouveau protocole basé sur l'utilisation d'états leurres [Hwang 2003][Lo 2005] résiste très bien aux attaques PNS et permet aux implémentations par laser atténué de conserver de bonnes performances en terme de distance accessible.

3.3 Équivalence entre modèle intriqué et modèle P&M

3.3.1 Modèle intriqué

Les protocoles présentés précédemment sont en général implémentés dans le modèle dit "Prepare and Measure" (P&M) où Alice prépare un état quantique à partir de ses choix de bits et le transmet à Bob qui le mesure dans une base choisie aléatoirement. Cette méthode permet de réaliser des protocoles de distribution quantique de clés avec la technologie actuellement disponible et ne nécessite pas de matériels

complexes tels qu'une source de photons intriqués ou une mémoire quantique.

Il existe une autre méthode permettant de réaliser des protocoles de distribution quantique de clés et utilisant des paires intriquées. Ces protocoles appelés "Entanglement Based" (EB) ont été introduits pour la première fois dans [Ekert 1991] et [Bennett 1992b].

Dans ce modèle, au lieu de préparer un état quantique à une particule, Alice prépare un état bipartite intriqué et transmet ensuite à Bob la moitié de cet état. Après avoir mesuré dans une base choisie la partie qu'elle a conservé, l'état de Bob est projeté sur l'état correspondant à ce qu'Alice a mesuré.

Pour illustrer ce principe, on considère qu'Alice prépare un état de Bell qu'on peut écrire

$$|\phi\rangle_{AB} = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}. \tag{3.1}$$

Alice conserve la moitié de cet état et transmet à Bob l'autre moitié par l'intermédiaire du canal quantique. Avant la mesure d'Alice, l'état que reçoit Bob s'écrit

$$\rho_B = \mathrm{Tr}_A \, |\phi\rangle\langle\phi|_{AB} = \frac{\mathbb{I}_2}{2}. \tag{3.2}$$

Une fois Alice et Bob chacun en possession d'une moitié de la paire intriquée, ils peuvent mesurer leur état quantique dans une base choisie aléatoirement. Si les paires intriquées sont parfaites alors les résultats de mesure correspondants aux même bases sont parfaitement corrélés.

Une fois cette phase de communication quantique terminée, la phase de réconciliation classique se déroule comme pour les protocoles P&M : tamisage, correction d'erreur, estimation de paramètre et amplification de confidentialité.

Un des intérêts de ce modèle est de faciliter l'étude de la sécurité des protocoles associés comme nous le montrons dans les chapitres 4 et 5.

3.3.2 Méthode de passage d'un modèle à l'autre

Étant donné qu'il est plus facile d'étudier la sécurité des protocoles de distribution quantique de clés lorsqu'ils sont sous la forme EB, il est intéressant de noter qu'il est facile de transformer théoriquement un protocole de la forme EB à la forme P&M

Si on reprend l'exemple précédent, lorsqu'Alice choisit de mesurer son état dans la base b (base $\{0,1\}$ pour $b = 0$ et $\{+,-\}$ pour $b = 1$) et obtient le résultat $x \in \{0,1\}$, l'état ρ_B de Bob est alors projeté sur l'état pur $H^b |x\rangle$. On se retrouve alors dans les mêmes conditions que pour la version *Prepare and Measure* du protocole. En particulier, les statistiques classiques des mesures d'Alice et de Bob sont

identiques dans les deux modèles.

Une preuve de sécurité obtenue dans le modèle EB permet ainsi de prouver la sécurité de la version P&M du protocole, celle que la technologie actuelle permet d'implémenter.

3.4 Modèles de sécurité habituellement utilisés

Les protocoles de distribution quantique de clés visent à obtenir des clés inconditionnellement sûres. Cependant, les premières preuves de sécurité inconditionnelles ne sont apparues que des années après l'invention des premiers protocoles de distribution quantique de clés. La sécurité inconditionnelle de BB84 a par exemple été prouvée pour la première fois en 2000 [Shor 2000]. Pour certains protocoles, il n'existe pas encore à l'heure actuelle de preuves de sécurité inconditionnelles : c'est le cas par exemple pour le COW [Gisin 2004] ou le DPS [Inoue 2002]. Il était donc utile d'élaborer des modèles de sécurité restreints dans lesquels la sécurité des premiers protocoles de distribution quantique de clés a pu être étudiée.

Nous présentons dans les sous-sections suivantes les différents modèles de sécurité habituellement considérés du moins au plus général.

3.4.1 Attaques de type interception-réémission

Les attaques de type interception-réémission sont les premières à avoir été étudiées : déjà dans l'article fondateur de la cryptographie quantique [Bennett 1984], la sécurité du protocole BB84 face à un adversaire limité aux attaques de type interception-réémission était analysée.

Dans les attaques de type interception-réémission, l'espion se met tout simplement à la place de Bob et effectue une mesure dans une base qui peut ne pas être identique à celles de Bob. Par exemple, dans l'attaque d'interception-réémission dans la base intermédiaire [Bennett 1992a] également appelée attaque dans la base de Breidbart, l'espion mesure tous les qubits dans une même base intermédiaire entre les deux bases utilisées par Alice et Bob. L'espion peut également choisir de mesurer dans les même bases que celles utilisées par les participants honnêtes du protocoles, et c'est ce cas que nous allons détailler ici pour illustrer notre propos.

Si on reprend l'exemple du protocole BB84 décrit précédemment, un espion pratiquant une attaque de ce type choisit de mesurer les qubits envoyés par Alice dans une des deux bases $\{0, 1\}$ ou $\{+, -\}$ et de renvoyer à Bob le résultat de cette mesure. Il y a alors deux possibilités équiprobables :

- si la base choisie par l'espion correspond à la base choisie par Alice alors l'espion obtient toute l'information sur le bit secret ce qui permet à l'espion de renvoyer un état non perturbé à Bob.

- dans le cas contraire, l'espion n'obtient aucune information sur le bit secret et aura dans ce cas perturbé le qubit transféré à Bob.

En moyenne, cette attaque fournit à l'espion une connaissance parfaite de la moitié des bits secrets au prix de la création d'un taux d'erreur $Q = 25$ % entre Alice et Bob. Ainsi, l'information mutuelle entre l'espion et Alice est égale à $I_E = 0,5$ par qubit transmis.

En reprenant les résultats de [Csiszar 1978] sur la possibilité d'extraire une clé secrète, on rappelle que le taux de clé secrète t_{sec} peut s'écrire :

$$t_{sec} = \max[I(A:B) - I_E, 0]. \tag{3.3}$$

A partir du taux d'erreur obtenu précédemment, on peut calculer l'information mutuelle entre Alice et Bob : $I(A:B) = 1 - h(Q)$. Dans ce cas on a $I(A:B) < I_E$. On peut donc affirmer que si un espion attaque les communications quantiques d'Alice et Bob de cette façon, il n'est pas possible de générer une clé secrète.

Si maintenant l'espion attaque une fraction η des qubits transmis par Alice, alors le QBER [4] généré sur le canal Alice Bob est de $Q = \eta/4$ et la quantité d'information obtenue par l'espion n'est plus que de $I_E = \eta/2$. Dans ce cas, une clé peut être générée par Alice et Bob tant que l'espion attaque moins de 68 % des qubits (ce qui correspond à un QBER de 17 %).

L'intérêt principal de ces attaques est d'être facilement analysables et implémentables avec la technologie actuelle sur des dispositifs expérimentaux de distribution quantique de clés. L'analyse de ces attaques permet en général de mieux comprendre le principe de fonctionnement des protocoles de distribution quantique de clés.

Cependant un espion limité aux attaques de type interception-réémission est beaucoup plus faible qu'un espion limité seulement par les lois de la mécanique quantique : autrement dit le modèle de sécurité manque de généralité. Il est donc nécessaire d'introduire des modèles intermédiaires entre sécurité inconditionnelle et sécurité face aux attaques de type interception-réémission.

3.4.2 Modèle des attaques individuelles

La catégorie des attaques individuelles représente les attaques pour lesquelles l'espion a accès à une mémoire quantique mais dont les possibilités de manipulation

4. Quantum Bit Error Rate : taux d'erreur sur le canal Alice-Bob

des qubits sont limitées. Plus précisément, cette catégorie est caractérisée par les contraintes suivantes :

- l'espion peut attaquer chacun des qubits envoyés par Alice individuellement. On peut de plus considérer sans perte de généralité qu'il emploie la même stratégie pour tous les qubits : il a en effet tout intérêt à employer la plus avantageuse pour lui.

- l'espion doit mesurer l'ensemble des états quantique en sa possession avant le début de la correction d'erreur et de l'amplification de confidentialité. Il peut par contre attendre la phase de tamisage et donc la révélation des bases pour faire ses mesures.

La première contrainte se traduit mathématiquement par une forme particulière de l'état ρ_{AB} dans la forme entanglement-based des protocoles de distribution quantique de clés. Comme l'action de l'espion est identique sur chacune des paires de qubits intriqués, il est possible de factoriser ρ_{AB} sous la forme :

$$\rho_{AB} = (\sigma_{AB})^{\otimes n}. \tag{3.4}$$

Cela permet d'étudier la sécurité du protocole en considérant une seule paire intriquée au lieu de l'ensemble des paires échangées au cours de la phase de communication quantique.

La deuxième contrainte permet d'être assuré qu'Alice, Bob et Eve sont en possession d'une distribution classique de bits corrélés au début de la phase de réconciliation. Cela signifie qu'il est possible d'utiliser les résultats de [Csiszar 1978] sur le taux de clé secrète t_{sec} qu'il est possible de distiller :

$$t_{\text{sec}} = I(A:B) - \max_{\text{Att. Ind.}} I(A:E), \tag{3.5}$$

où la maximisation est faite sur l'ensemble des attaques individuelles réalisables par l'espion.

Ce modèle d'attaque est suffisamment simple pour permettre de décrire explicitement les attaques optimales comme par exemple dans [Lütkenhaus 1999] pour BB84. Ces descriptions explicites permettent de mieux comprendre les mécanismes du protocole à l'origine de la sécurité et peuvent faciliter l'analyse dans les modèles de sécurité plus généraux.

Calcul du taux de clé secrète dans le cas particulier de BB84.

Nous reprenons la méthode utilisée dans [Gisin 2002] pour décrire l'attaque individuelle optimale sur BB84. Dans le chapitre 5 page 104 nous généralisons cette méthode au cas où la mémoire utilisée par l'espion est bruitée. Nous reprenons ici les résultats obtenus dans le cas particulier où le bruit p dans la mémoire est fixé à 0.

Ainsi, pour un QBER sur le canal Alice/Bob Q, la probabilité $p_{\text{dev.}}$ que l'espion devine correctement le bit secret est :

$$p_{\text{dev.}} = \frac{1}{2} + \sqrt{Q(1-Q)}. \tag{3.6}$$

On peut alors calculer les deux termes de l'équation 3.5. En reprenant les notations de cette équation on a :

$$I(A:B) = 1 - h(Q) \tag{3.7}$$

$$\max_{\text{Att. Ind.}} I(A:E) = 1 - h(p_{\text{dev.}}) = 1 - h(\frac{1}{2} + \sqrt{Q(1-Q)}). \tag{3.8}$$

Le taux de clé secrète $t_{\text{sec}} = h(\frac{1}{2} + \sqrt{Q(1-Q)}) - h(Q)$ est donc une fonction décroissante du QBER qui s'annule lorsque $Q = \frac{\sqrt{2}-1}{2\sqrt{2}} \approx 14,6\ \%$.

Cela signifie que pour un adversaire limité aux attaques individuelles, Alice et Bob peuvent utiliser BB84 pour distiller une clé secrète tant que le QBER mesuré sur le canal quantique est inférieur à $14,6\ \%$.

3.4.3 Modèle des attaques collectives

Les attaques collectives sont une généralisation des attaques individuelles où l'espion a la possibilité d'attendre la fin de la phase de réconciliation pour effectuer ses mesures. Ce modèle introduit pour la première fois dans [Biham 1997] est caractérisé par les contraintes suivantes sur les actions de l'espion :

- comme pour les attaques individuelles, l'espion emploie la même stratégie d'attaque sur chacun des qubits envoyés par Alice.

- l'espion peut attendre la fin de la phase de réconciliation (ou plus longtemps encore, comme par exemple après qu'Alice et Bob aient utilisé leur clé dans un autre protocole) avant de mesurer ses états quantiques et peut utiliser une mesure cohérente sur l'ensemble des états quantiques en sa possession s'il le souhaite.

Sous ces contraintes, le taux de clé secrète qu'il est possible de distiller contre un adversaire limité aux attaques collectives est donné par la borne de Devetak-Winter [Devetak 2005]. On peut ainsi écrire :

$$t_{\text{sec}} = I(A:B) - \max_{\text{Att. Coll.}} \chi(A:E), \tag{3.9}$$

où la maximisation est faite sur l'ensemble des attaques collectives et $\chi(A:E)$ représente la quantité de Holevo telle que nous l'avons définie dans le premier chapitre page 30.

Ce modèle est très général et dans certains cas les bornes de sécurité obtenues sont même optimales : c'est le cas par exemple de BB84 pour lequel les attaques collectives apportent autant d'information à l'espion que les attaques les plus générales autorisées par la mécanique quantique [Kraus 2005].

Calcul du taux de clé secrète dans le cas particulier de BB84.

En reprenant l'expression de la quantité de Holevo $\chi(A:E)$ définie dans le premier chapitre, on a :

$$\chi(A:E) = H(\rho_E) - \sum_x p(x) H(\rho_E^x) \tag{3.10}$$

où ρ_E^x représente l'état d'Eve lorsque le bit secret d'Alice est x. En reprenant ici les résultats obtenus dans le chapitre 4 page 76, il est possible de calculer explicitement cette quantité en fonction du QBER sur le canal Alice/Bob noté Q. On a alors :

$$\chi(A:E) = h(Q) \tag{3.11}$$

et donc

$$t_{\text{sec}} = 1 - 2h(Q). \tag{3.12}$$

En utilisant BB84, Alice et Bob peuvent donc distiller une clé secrète contre un adversaire non limité tant que le QBER sur le canal quantique est inférieur à 11 %.

3.4.4 Modèle des attaques cohérentes

Le modèle des attaques cohérentes ne contraint les actions de l'espion d'aucune manière mis à part le respect des lois de la mécanique quantique. Ainsi, l'espion peut éventuellement intriquer plusieurs qubits envoyés par Alice entre eux ou adapter sa stratégie en cours de protocole en fonction des résultats de ses mesures.

Les possibilités sont trop nombreuses pour pouvoir être listées et encore moins être paramétrées. Il est donc impossible d'optimiser les attaques cohérentes sur l'ensemble des possibilités.

Il est néanmoins possible de prouver la sécurité de certains protocoles contre ces attaques les plus générales : c'est le cas par exemple de BB84 pour lequel il a été prouvé [Renner 2005a] que les attaques collectives sont équivalentes aux attaques cohérentes.

3.5 Utilité de nouveaux modèles de sécurité

Nous venons de présenter les modèles de sécurité habituels dans lesquels la sécurité des protocoles de distribution quantique de clés est étudiée. Dans les sous sections suivantes, nous exposons les raisons qui nous ont incités à étudier de nouveaux modèles de sécurité pour les protocoles de distribution quantique de clés.

3.5.1 Un modèle réaliste

Dans les trois modèles de sécurité des attaques individuelles, collectives et cohérentes, l'adversaire est supposé avoir accès à une mémoire quantique. Pourtant, comme nous l'expliquons au début du chapitre 5, cette technologie n'est pas encore disponible en quantité et en qualité suffisante pour la réalisation pratique des attaques sur les protocoles de distribution quantique de clés. Il est donc intéressant de connaître l'évolution des bornes de sécurité des protocoles de distribution quantique de clés lorsque l'adversaire est limité par la qualité de sa mémoire.

Nous notons ici que cette supposition d'une mémoire imparfaite est une estimation liée à une technologie dont l'évolution est prévisible. Cela est très différent par exemple de la difficulté supposée de la factorisation des grands nombres. Il est possible a priori que l'invention d'un nouvel algorithme permette du jour au lendemain d'améliorer les possibilités de factorisation d'un attaquant. Il est par contre beaucoup moins probable qu'une technologie de mémoire quantique parfaite émerge sur la même échelle de temps.

C'est en ce sens que nous affirmons que ce modèle de sécurité est réaliste et ancré sur des limitations technologiques étudiées et comprises.

3.5.2 Amélioration des performances

Un des avantages espérés de la dégradation de la puissance de l'espion est une amélioration des performances des protocoles de distribution quantique de clés. Ces améliorations de performance peuvent être de deux types : une augmentation du taux d'erreur critique sur le canal quantique au delà duquel il n'est pas possible de distiller une clé ou une augmentation du taux de clé secrète.

Nos travaux ont permis de quantifier ces améliorations de performances en fonction du bruit de la mémoire de l'adversaire. Cela permet aux participants honnêtes

de mesurer précisément le compromis qu'ils peuvent faire entre la sécurité du protocole et les performances espérées.

Meilleure est leur connaissance de la qualité de la mémoire quantique de l'espion, meilleures seront les performances du protocoles de distribution quantique utilisé.

3.5.3 Développement du *quantum hacking*

Depuis quelques années s'est développé un domaine de recherche sur les protocoles de distribution quantique de clés appelé le *quantum hacking*. Ces techniques visent à contourner les preuves de sécurité des systèmes de distribution quantique de clés en s'attaquant directement aux défauts d'implémentation.

Des techniques telles que l'éblouissement des détecteurs [Lydersen 2010] permettent de compromettre gravement la sécurité des clés produites par un système de distribution quantique de clés sans que les participants honnêtes puissent s'en rendre compte facilement. Alors même que le protocole théorique est inconditionnellement sûr, dans certains cas des défauts d'implémentation peuvent permettre à un adversaire d'avoir une connaissance parfaite du secret.

Si la sécurité est une chaîne, alors on peut dire que le maillon faible est actuellement l'implémentation physique des protocoles. Dans ce cas il n'est pas déraisonnable de se contenter d'une sécurité contre un adversaire limité par la qualité de sa mémoire pour la sécurité théorique du protocole, un autre maillon de la chaîne.

Grâce à cette dégradation de la puissance de l'espion, on peut alors espérer récupérer tout ou partie des performances perdues du fait de l'installation de contremesures sur l'implémentation du protocole.

Chapitre 4

Attaques optimales sans mémoire

Sommaire

Dans ce chapitre, nous allons présenter les résultats obtenus sur les attaques optimales sans mémoire appliquées aux protocoles de distribution quantique de clés.

Cette étude est motivée par deux raisons principales :

- un modèle réaliste : comme nous l'avons déjà évoqué à la fin du chapitre précédent, les modèles de sécurité traditionnels que sont les modèle des attaques individuelles, collectives et cohérentes nécessitent une mémoire quantique. Cette technologie est pourtant loin d'être disponible à l'heure actuelle, comme nous le démontrons au début du chapitre 5. Les attaques réalistes aujourd'hui sont donc limitées par une mémoire quantique au mieux bruitée et en quantité limitée. A l'extrême, les attaques réellement implémentables avec la technologie actuelle n'utilisent pas de mémoire quantique. Il est donc

intéressant d'étudier les attaques optimales sans mémoire quantique.

- une étape indispensable pour la preuve de sécurité dans le modèle de la mémoire quantique bruitée : les résultats de l'optimisation des attaques sans mémoire sont utilisés dans le modèle de la mémoire bruitée étudié dans le chapitre suivant. Ces résultat n'existant pas dans la littérature pour les protocoles six-states et SARG04, il était nécessaire de déterminer les attaques optimales sans mémoire pour ces deux protocoles avant de poursuivre l'étude de leur sécurité dans le modèle de la mémoire bruitée.

Après une revue des principaux résultats connus sur le sujet, nous présentons le principe général du modèle sans mémoire dans une deuxième section, puis nous présentons l'attaque optimale ainsi que les résultats en terme de borne de sécurité dans les sections suivantes.

4.1 Travaux existants sur le sujet

Historiquement, les toutes premières études de sécurité des protocoles de distribution quantique de clés ont été basées sur des attaques simples ne nécessitant pas de mémoire quantique : les attaques de type interception/réémission. C'est le cas par exemple dans [Bennett 1984] où une attaque d'interception/réémission dans les bases de BB84 est décrite. Cette étude permet de déterminer une première borne supérieure sur le taux d'erreur acceptable sur le canal quantique entre Alice et Bob, le taux d'erreur qui est généré lorsqu'un espion se place entre Alice et Bob et mesure l'ensemble des états quantiques transférés. Il est possible d'améliorer ces attaques en choisissant une base de mesure différente pour l'espion. C'est ce qui a été proposé dans [Bennett 1992a] avec une attaque de type interception/réémission dans la base intermédiaire ou base de Breidbart pour laquelle l'ensemble des états quantique mesurés par Alice sont mesurés dans une même base.

Ces attaques constituent en général la première analyse de sécurité d'un protocole de distribution quantique de clés en raison de leur simplicité mais ne sont pas assez générales pour représenter un espion limité par l'absence de mémoire quantique. Ce cas plus général des attaques optimales sans mémoire a été étudié par [Lütkenhaus 1996] sur le protocole BB84.

Nous avons eu connaissance de ces travaux après avoir développé les outils permettant la détermination des attaques optimales sans mémoire sur les protocoles BB84, SARG04 et *six-states* grâce à une optimisation numérique de l'ensemble des paramètres de l'attaque de l'espion. En découvrant les résultats de [Lütkenhaus 1996] dont l'étude ne portait que sur le protocole BB84, nous nous sommes aperçus que les résultats de notre optimisation numérique étaient en accord avec les résultats obtenus avec une méthode différente.

La méthode utilisée par [Lütkenhaus 1996] se base en effet sur la version $P\&M$ de BB84 : l'attaque d'Eve est caractérisée par un POVM appliqué directement au qubit envoyé par Alice. Après une optimisation analytique de ce POVM, cette méthode aboutit à une formule littérale de l'information mutuelle entre Alice et Eve pour un taux d'erreur sur le canal quantique donné.

Nous avons de notre côté étudié la version équivalente de cette attaque dans le modèle intriqué équivalent de BB84. L'attaque d'Eve est optimisée à la fois sur l'interaction entre le qubit envoyé par Alice et le système quantique auxiliaire de l'espion et sur la mesure effectuée sur ce système auxiliaire.

Malgré l'ancienneté de ces résultats concernant BB84 dans le modèle sans mémoire, il n'existe pas à notre connaissance de travaux sur les attaques optimales sans mémoire pour les protocoles *six-states* et SARG04. Nous avons donc appliqué notre méthode à ces deux protocoles de distribution quantique de clés pour déterminer les bornes de sécurité contre un adversaire sans mémoire quantique.

On peut également évoquer [Bechmann-Pasquinucci 2006] dont l'étude concerne les attaques sans mémoire sur BB84. Dans le modèle d'espion considéré dans cet article, la taille du système quantique auxiliaire utilisé par l'espion est limitée à un seul qubit au lieu du système décrit par un espace de Hilbert de dimension 4 qui doit être considéré en toute généralité. Cette analyse ne permet donc pas d'atteindre les performances de l'attaque optimale sans mémoire décrite dans [Lütkenhaus 1996] et que nous retrouvons grâce à notre méthode.

4.2 Principe de l'attaque

4.2.1 Principe général et restrictions imposées à l'espion

On considère un protocole de distribution quantique de clés entre deux participants Alice et Bob. Au cours de la phase quantique, Alice choisit d'encoder un message sur un état quantique et le transmet à Bob qui effectue une mesure sur cet état et stocke le résultat dans une mémoire classique.

Dans le modèle de sécurité considéré, on suppose que l'espionne Eve n'a pas accès à une mémoire quantique mais qu'en dehors de cela n'est pas limitée en capacité de calcul ou de mémoire classique. Ainsi, en tenant compte de ces limitations, Eve peut en tout généralité effectuer les actions suivantes au cours de la phase quantique du protocole :

1. Elle réalise une opération unitaire U de son choix entre le qubit envoyé par Alice et un système auxiliaire qu'elle conserve dans son laboratoire.

2. Sans attendre, Eve peut alors mesurer ce système auxilaire grâce à un POVM et stocker le résultat dans une mémoire classique.

3. Pendant la phase de réconciliation lorsque l'information de la base utilisée par Alice est annoncée Eve utilise cette information en plus du résultat de sa mesure pour optimiser son information sur le bit secret.

4.2.2 Description de l'attaque

Dans le modèle *Prepare and Measure*

A partir de maintenant, afin d'illustrer notre propos, nous considérons qu'Alice et Bob utilisent le protocole BB84. Ainsi, dans le modèle *Prepare and Measure*, Alice choisit un bit secret x et une base b qui prennent leurs valeurs dans l'ensemble $\{0,1\}$ et fabrique l'état $|a\rangle = H^b |x\rangle$ (où H représente la transformation de Hadamard) avant de l'envoyer à Bob.

On considère alors l'interaction la plus générale que peut effectuer Eve entre le qubit d'Alice et un système auxiliaire. On note $|0\rangle_E$ l'état initial du système auxiliaire utilisé par Eve. L'état du système juste avant l'interaction d'Eve est donc décrit par l'état quantique

$$|\Phi\rangle_{\text{init}} = |a\rangle \otimes |0\rangle_E . \tag{4.1}$$

En toute généralité, Eve peut appliquer une opération unitaire notée U à ce système afin d'intriquer son système auxiliaire au qubit voyageant entre Alice et Bob. Ce faisant Eve introduit une perturbation sur le canal Alice/Bob qui sera mesurée par une augmentation du QBER. Plus l'intrication est forte, plus la quantité d'information que peut espérer récupérer Eve est grande au prix d'une perturbation plus importante du canal Alice/Bob. Ainsi, pour un QBER donné qu'Eve se permet de créer sur le canal quantique, elle n'a accès qu'à une partie de l'ensemble des opérations unitaires possibles. La détermination de ce sous-ensemble ainsi que l'optimisation du choix de l'interaction seront l'objet des sections suivantes.

Une fois l'opération unitaire effectuée, Eve n'ayant pas de mémoire quantique doit immédiatement mesurer son système avec un POVM de son choix. L'état quantique représentant le système d'Eve juste avant la mesure est

$$\rho_E = \mathrm{Tr}_A \left[U(|a\rangle\langle a| \otimes |0\rangle\langle 0|_E) U^\dagger \right] . \tag{4.2}$$

Après avoir mesuré son état quantique, Eve stocke le résultat dans une mémoire classique. Ce résultat ainsi que l'information classique sur la base utilisée par Alice qui est annoncée par la suite sont utilisés pour déterminer la valeur du bit secret. On

peut représenter l'ensemble de l'attaque d'Eve dans le modèle *Prepare and Measure* par le circuit quantique suivant :

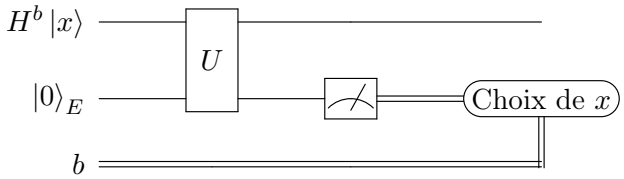


FIGURE 4.1 – Circuit quantique représentant l'attaque d'Eve dans le modèle *Prepare and Measure* du protocole de distribution quantique de clés BB84

Cette représentation est proche de ce que serait une implémentation réelle de l'attaque sur un système de distribution de clés déployé. Cependant, pour étudier la sécurité de ce protocole, on utilise un modèle équivalent produisant les mêmes statistiques chez Alice, Bob et Eve appelé modèle intriqué équivalent.

Modèle intriqué équivalent.

Dans ce modèle, au lieu de préparer un état quantique à une particule, Alice prépare un état bipartite intriqué et transmet ensuite à Bob la moitié de cet état. Après avoir mesuré dans une base choisie la partie qu'elle a conservé, l'état de Bob est projeté sur l'état correspondant à ce qu'Alice a mesuré.

Dans notre cas, Alice prépare l'état de Bell

$$|\phi\rangle_{AB} = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}} \tag{4.3}$$

et envoie l'état

$$\rho_B = \mathrm{Tr}_A \, |\phi\rangle\langle\phi|_{AB} = \frac{\mathbb{I}_2}{2} \tag{4.4}$$

à Bob (c'est l'état complètement mixte). Alice choisit alors de mesurer son état dans une base b ($\{0,1\}$ pour $b = 0$ et $\{+,-\}$ pour $b = 1$) et obtient alors le résultat $x \in \{0,1\}$. L'état ρ_B de Bob est alors projeté sur l'état pur $H^b |x\rangle$. On se retrouve alors dans les mêmes conditions que pour la version *Prepare and Measure* du protocole. En particulier, les statistiques classiques des mesures d'Alice et de Bob sont identiques dans les deux modèles.

L'intérêt de ce modèle équivalent est que la sécurité du protocole est plus facile à étudier lorsqu'il est dans le modèle intriqué équivalent. C'est la méthode que nous employons dans la suite de cette section. L'équivalence que nous venons de prouver nous assure qu'une preuve de sécurité obtenue dans ce modèle intriqué équivalent

implique automatiquement la preuve de sécurité du protocole en version *Prepare and Measure*.

Dans ce modèle, l'action d'Eve sur le canal Alice/Bob est caractérisée par le canal équivalent appliqué à $|\phi\rangle_{AB}$. Ainsi, l'état ρ_{AB} partagé par Alice et Bob après l'action d'Eve s'écrit

$$\rho_{AB} = \mathcal{E}(|\phi\rangle\langle\phi|_{AB}) \tag{4.5}$$

où ρ_{AB} n'est plus a priori un état pur après application du bruit généré par l'attaque d'Eve.

Dans le modèle intriqué équivalent, l'information accessible à Eve est entièrement contenue dans la purification de l'état ρ_{AB}. Ainsi, si on note $\rho_{ABE} = |\psi\rangle\langle\psi|_{ABE}$ cette purification, Eve a accès à l'information contenue dans le système $\rho_E = \mathrm{Tr}_{AB}\rho_{ABE}$.

Dans la section suivante, une paramétrisation de cette purification permettra d'optimiser l'information mutuelle entre Alice et Eve.

4.3 Optimisation de l'attaque

4.3.1 Paramétrisation de l'interaction entre les systèmes d'Alice et d'Eve

Dans cette sous-section, la paramétrisation de l'attaque d'Eve est faite à partir du modèle intriqué équivalent du protocole. Les états bipartites ρ_{AB} à considérer doivent obéir à des contraintes permettant de limiter grandement les degrés de liberté accessibles à Eve.

Pour caractériser les états ρ_{AB} à considérer, on reprend un résultat démontré dans [Kraus 2005] et [Renner 2005b] qui nous assure que la sécurité de BB84 peut être étudiée sans perte de généralité en considérant les attaques pour lesquelles la matrice ρ_{AB} est diagonale dans la base de Bell. Cela signifie que ρ_{AB} s'écrit simplement sous la forme

$$\begin{aligned} \rho_{AB} \quad = \quad & \alpha \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \beta \left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \gamma \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \delta \left|\Psi^-\right\rangle\left\langle\Psi^-\right| \\ & \text{avec} \quad \alpha + \beta + \gamma + \delta = 1, \end{aligned} \tag{4.6}$$

où $|\Phi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$ et $|\Psi^\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$ sont les états de Bell.

En plus de la condition de normalisation $\mathrm{Tr}\,\rho_{AB} = 1$, l'estimation du QBER effectuée par Alice et Bob pendant la phase de réconciliation du protocole ajoute des contraintes sur les coefficients de ρ_{AB}. Ainsi, si on note respectivement Q_0 et

Q_1 les QBER mesurés par Alice et Bob dans les bases $\{|0\rangle, |1\rangle\}$ et $\{|+\rangle, |-\rangle\}$ alors on obtient les relations

$$\begin{aligned} Q_0 &= \langle 01| \rho_{AB} |01\rangle + \langle 10| \rho_{AB} |10\rangle = \gamma + \delta, \\ Q_1 &= \langle +-| \rho_{AB} |+-\rangle + \langle -+| \rho_{AB} |-+\rangle = \beta + \delta. \end{aligned} \tag{4.7}$$

Si les QBER mesurés sur les 2 bases sont différents, cela est un signe pour Alice et Bob que le canal quantique a pu être manipulé par un attaquant. Dans ce cas, ils peuvent soit choisir d'abandonner la session du protocole et repartir de zéro soit choisir $Q = \max(Q_0, Q_1)$ comme valeur de QBER pour le reste de la réconciliation. Dans les deux cas, Eve a alors tout intérêt à choisir une attaque pour laquelle on a $Q_0 = Q_1 = Q$.

Avec ces deux contraintes supplémentaires, l'état ρ_{AB} ne dépend plus que de $Q \in [0, 1/2]$ et d'un paramètre libre $\alpha \in [1 - 2Q, 1 - Q]$ avec la relation

$$\begin{aligned} \rho_{AB} &= \alpha \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + (1 - Q - \alpha) \left|\Phi^-\right\rangle\left\langle\Phi^-\right| && (4.8) \\ &\quad + (1 - Q - \alpha) \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + (2Q - 1 + \alpha) \left|\Psi^-\right\rangle\left\langle\Psi^-\right|. && (4.9) \end{aligned}$$

Pour mesurer la quantité d'information accessible à l'espionne dans ce modèle on utilise le fait que toute l'information est contenue dans une purification $|\psi\rangle\langle\psi|_{ABE}$ de ρ_{AB}. Eve est en possession de la partie ρ_E de cette purification avec

$$\rho_E = \mathrm{Tr}_{AB} |\psi\rangle\langle\psi|_{ABE}. \tag{4.10}$$

À partir de 4.8 il est facile de trouver une purification de ρ_{AB}. En effet, on voit que

$$\begin{aligned} |\psi\rangle_{ABE} &= \sqrt{\alpha} \left|\Phi^+\right\rangle_{AB} \left|\Phi^+\right\rangle_E + \sqrt{1 - Q - \alpha} \left|\Phi^-\right\rangle_{AB} \left|\Phi^-\right\rangle_E \\ &\quad + \sqrt{1 - Q - \alpha} \left|\Psi^+\right\rangle_{AB} \left|\Psi^+\right\rangle_E \\ &\quad + \sqrt{2Q - 1 + \alpha} \left|\Psi^-\right\rangle_{AB} \left|\Psi^-\right\rangle_E. \end{aligned} \tag{4.11}$$

vérifie bien l'équation $\mathrm{Tr}_E |\psi\rangle\langle\psi|_{ABE} = \rho_{AB}$ et est donc bien une purification de ρ_{AB}. Il y a une infinité de purifications possibles mais elles sont reliées par une relation unitaire. On peut donc en choisir une en particulier sans perte de généralité puisque Eve peut toujours choisir d'appliquer cette opération unitaire.

À partir de cette purification, il est possible de calculer l'état quantique dont dispose Eve après l'interaction avec le qubit d'Alice. Ainsi, lorsqu'Alice mesure son état dans la base b et obtient le résultat x l'état quantique d'Eve que l'on note ρ_E^{xb} s'écrit après normalisation

$$\rho_E^{xb} = \frac{\mathrm{Tr}_{AB}[(H^b |x\rangle\langle x| H^b \otimes \mathbb{I}_B \otimes \mathbb{I}_E)\rho_{ABE}]}{\mathrm{Tr}[(H^b |x\rangle\langle x| H^b \otimes \mathbb{I}_B \otimes \mathbb{I}_E)\rho_{ABE}]} \tag{4.12}$$

où $\rho_{ABE} = |\psi\rangle\langle\psi|_{ABE}$ est une purification de ρ_{AB}.

L'état quantique accessible à Eve après interaction avec le qubit d'Alice est donc paramétré par le QBER sur le canal Alice/Bob noté $Q \in [0, 1/2]$ et par α dont la valeur peut être arbitrairement choisie par Eve dans l'intervalle $[1-2Q, 1-Q]$.

4.3.2 Paramétrisation de la mesure d'Eve

Après son action sur le qubit d'Alice, Eve se retrouve en possession de l'état quantique ρ_E^{xb} et doit immédiatement mesurer cet état avec un POVM qui maximise ses chances d'obtenir la valeur du bit x choisi par Alice sachant que la valeur du bit b (choix de la base utilisée par Alice) sera révélée par la suite une fois la mesure effectuée. Ce problème de discrimination des états quantiques a été largement étudié dans le cas général [Helstrom 1969, Chefles 2000]. Le cas particulier où de l'information classique est révélée après la mesure a été étudié dans [Ballester 2008].

Dans cet article sur les méthodes de discrimination d'états en présence d'information postérieure à la mesure, l'objectif est similaire au sujet qui nous intéresse. En effet, cet article considère le cas d'un jeu entre deux participants Alice et Bob dans lequel l'objectif de Bob est de deviner un bit secret encodé par Alice dans un état quantique. Plus précisément, Alice choisit aléatoirement deux bits secret qu'on note x et b et transmet à Bob un état quantique $|\phi\rangle_A^{xb}$ qui dépend à la fois de x et b. Bob doit déterminer la meilleure façon de déterminer la valeur de x sachant qu'Alice lui dévoilera la valeur de b une fois la mesure effectuée.

A l'aide d'une optimisation numérique, on trouve que la mesure optimale pour Bob dans ce cas consiste à utiliser un POVM à 4 éléments qu'on peut noter $\{M_{x_0x_1}\}_{x_0x_1=00,01,10,11}$ dont le résultat de mesure est x_0x_1. La révélation du choix du bit b par Alice permet alors à Bob de choisir le bit x_b comme estimation du choix x d'Alice. C'est cette méthode qui permet de maximiser la probabilité pour Bob de deviner correctement le bit secret d'Alice.

On peut reprendre cette technique pour décrire la méthode utilisée par Eve pour discriminer les états quantiques ρ_E^{xb}. Il s'agit de choisir le POVM qui maximise l'information mutuelle entre Alice et Eve avec la connaissance du bit b. Pour atteindre cet objectif, Eve choisit un POVM à 4 éléments qu'on peut noter $\{M_{x_0x_1}\}_{x_0x_1=00,01,10,11}$. Pour chaque mesure, Eve obtient 2 bits d'information x_0 et x_1 et attend la révélation du choix de base b pour décider de conserver le bit x_b correspondant. Cette stratégie permet d'utiliser au mieux l'information classique postérieure à la mesure.

Pour que $\{M_{x_0x_1}\}_{x_0x_1=00,01,10,11}$ forme un POVM, certaines propriétés doivent être vérifiées :

- les matrices M_i sont des opérateurs hermitiens semi-définis positifs ($M_i \geq 0$),
- $\sum_i M_i = \mathbb{I}$.

Une fois ces conditions vérifiées, on peut calculer les probabilités d'obtenir un certains résultat k lorsqu'Eve mesure l'état ρ_E^{xb} dans ce POVM :

$$p(K = k|X = x, B = b) = Tr(M_k \rho_E^{xb}). \tag{4.13}$$

Ces probabilités de mesure sont utilisées dans la sous-section suivante pour calculer l'information mutuelle entre Alice et Eve.

4.3.3 Maximisation de l'information mutuelle entre Alice et Eve

Après la phase de réconciliation, Eve est en possession de l'information B de la base utilisée par Alice et du résultat K de sa mesure sur son système auxiliaire. L'information mutuelle $I(X : KB)$ peut donc s'écrire

$$\begin{aligned} I(X : KB) &= H(X) + H(KB) - H(XKB) \\ &= 1 + H(K|B) + H(B) - H(K|XB) - H(XB) \\ &= H(K|B) - H(K|XB) \end{aligned} \tag{4.14}$$

où le passage de la première à la deuxième ligne s'obtient par la définition de l'entropie conditionnelle et le passage de la deuxième à la troisième ligne s'obtient en en remarquant que $H(X|B) = H(X) = 1$. En effet, X et B sont indépendants puisque choisis aléatoirement par Alice.

On peut alors calculer les entropies conditionnelles $H(K|B)$ et $H(K|XB)$ en fonction des probabilités conditionnelles obtenues à l'équation 4.13 :

$$\begin{aligned} H(K|XB) &= \sum_{x,b} p(X = x, B = b).H(K|X = x, B = b) \\ &= \frac{1}{4} \sum_{k,x,b} \Lambda[p(K = k|X = x, B = b)] \end{aligned} \tag{4.15}$$

$$\tag{4.16}$$

$$\text{et} \quad H(K|B) = \frac{1}{2} \sum_{k,b} \Lambda[p(K = k|B = b)] \tag{4.17}$$

où on a introduit la fonction $\Lambda(\cdot)$ définie par

$$\Lambda \ : \ x \longrightarrow \left| \begin{array}{cc} -x\log_2(x) & \text{si } x > 0 \\ 0 & \text{si } x = 0 \end{array} \right. \tag{4.18}$$

4.3.4 Calcul du taux de clé secrète

Dans ce modèle d'attaque sans mémoire, Eve ne peut pas conserver d'état quantique pendant l'exécution du protocole et doit mesurer immédiatement tout système auxiliaire utilisé. Cela signifie qu'au début de la phase de réconciliation, Alice, Bob et Eve sont chacun en possession d'une chaîne de bits classique. Nous sommes donc dans le cas d'application du résultat de Csiszár et Körner [Csiszar 1978]. Cela nous assure qu'après la phase d'amplification de confidentialité, une clé de taille l peut être extraite des chaînes de bits corrélées d'Alice et Bob avec

$$\begin{aligned} l &= I_{AB} - \max_{\text{stratégies}} I_{AE} \\ &= n[I(X:Y) - \max_{\text{stratégies}} I(X:KB)], \end{aligned} \tag{4.19}$$

où la maximisation est faite sur l'ensemble des stratégies d'attaques d'Eve, c'est à dire l'ensemble des interactions et des POVMs.

L'information mutuelle $I(X:Y)$ entre Alice et Bob se calcule facilement en fonction du taux d'erreur (le QBER noté Q) observé

$$I(X:Y) = H(X) - H(X|Y) = 1 - h(Q), \tag{4.20}$$

avec $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ la fonction entropie binaire.

En rassemblant les résultats, on trouve que le taux de clé secrète $r = \frac{l}{n}$ peut se calculer avec l'équation

$$r = 1 - h(Q) - \max_{strategies}[H(K|B) - H(K|XB)]. \tag{4.21}$$

Pour un QBER donné sur le canal Alice Bob, la maximisation se fait sur l'ensemble des POVM $\{M_i\}$ et sur l'ensemble des valeurs possibles de α, le paramètre caractérisant l'interaction entre le qubit d'Alice et le système d'Eve (voir 4.11). Ce problème d'optimisation peut être résolu numériquement en utilisant le *Semidefinite Programming* [Vandenberghe 1994] sous MATLAB. Pour cela les logiciels CVX [Grant 2008, Grant 2011] et SDPT3 [Toh 1999] ont été utilisés.

Une partie du code MATLAB réalisant cette optimisation est présenté et commenté en annexe page 139. Les résultats de ces optimisations permettent de tracer les courbes de taux de secret données dans la section suivante.

Notons également ici que cette méthode d'optimisation est réutilisée dans le chapitre suivant pour la preuve de sécurité de BB84 dans le modèle de la mémoire bruitée. Dans cette optique, on note $\kappa(Q)$ le résultat de l'optimisation suivante :

$$\kappa(Q) = \min_{strategies} H(K|XB). \tag{4.22}$$

4.4 Bornes de sécurité

4.4.1 BB84

Le calcul du taux de clé secrète obtenu avec le protocole BB84 a été fait dans la section précédente. Nous pouvons alors tracer sur la figure 4.2 le résultat de l'optimisation de l'information mutuelle entre Alice et Eve sur l'ensemble des interactions et des POVMs utilisables.

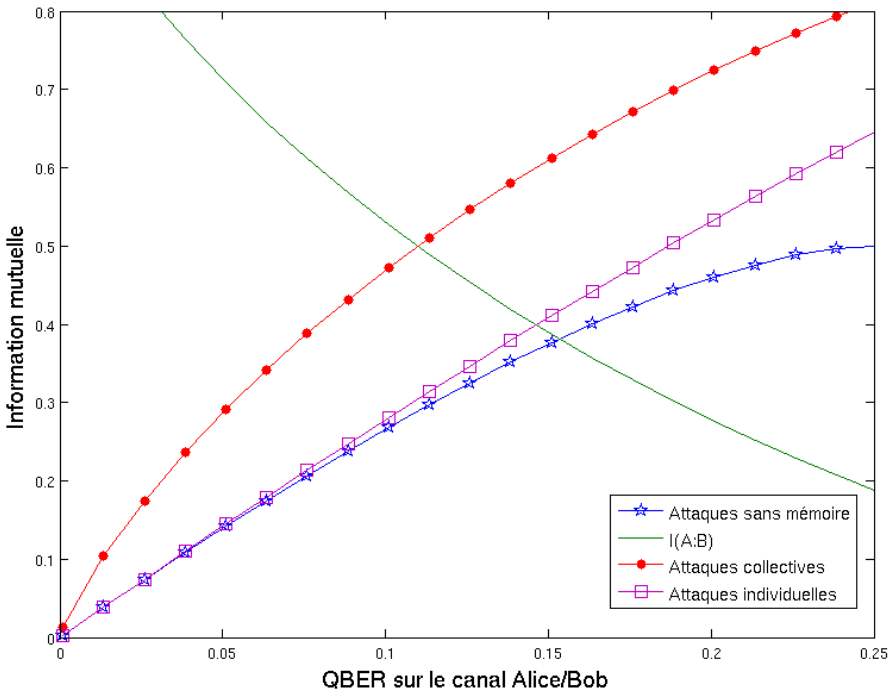


FIGURE 4.2 – Information mutuelle entre Alice et Bob et entre Alice et Eve pour BB84 dans différents modèles de sécurité.

On peut observer sur la figure 4.2 que dans le modèle d'attaque sans mémoire, Eve obtient comme prévu moins d'information que dans le cas des attaques individuelles (nécessitant l'utilisation d'une mémoire quantique) et a fortiori par rapport

aux attaques collectives.

Le taux de clé en fonction du QBER sur le canal Alice/Bob est tracé en figure 4.3. On peut observer que dans le modèle de l'attaque sans mémoire, une clé peut être générée pour un QBER inférieur à $15,4$ %, au lieu de 11 % pour les attaques collectives et $14,6$ % pour les attaques individuelles.

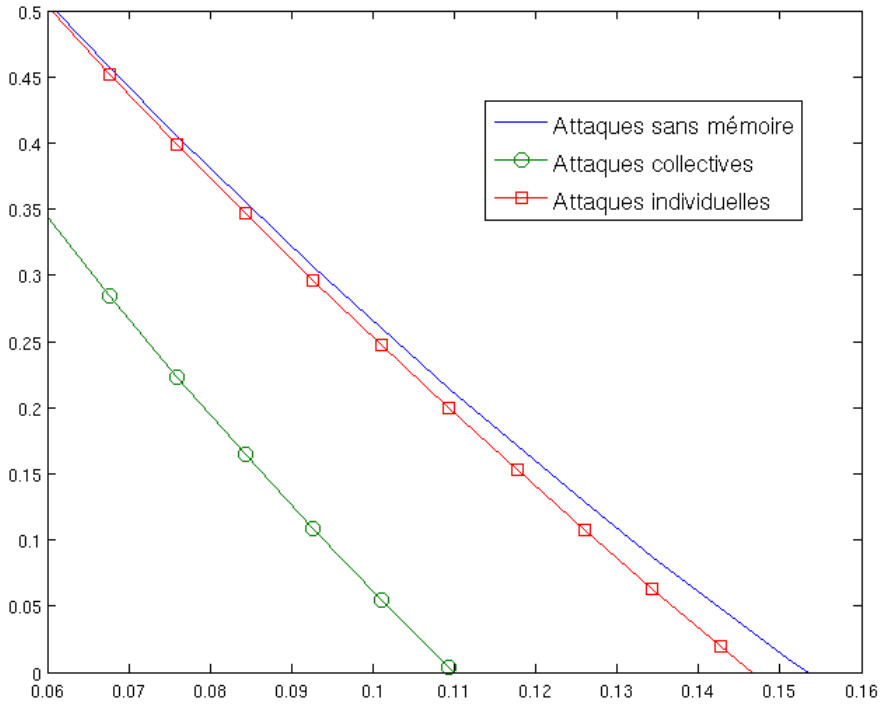


FIGURE 4.3 – Taux de clé secrète pour BB84 dans différents modèles de sécurité.

Cette attaque optimale sans mémoire obtenue par optimisation de l'attaque d'Eve dans le modèle intriqué équivalent de BB84 coïncide précisément avec un résultat déjà connu [Lütkenhaus 1996] obtenu en optimisant l'attaque d'Eve dans la version *Prepare and Measure* de BB84. Alors que notre résultat est obtenu par une optimisation numérique et que le taux de clé est donc connu numériquement, l'attaque explicite optimale développée dans [Lütkenhaus 1996] permet de calculer ce taux de clé secrète sous forme littérale.

Les deux méthodes aboutissent au même résultat pour l'information mutuelle entre Alice et Eve et cela nous permet donc d'obtenir une formule littérale pour le résultat de l'optimisation numérique de l'information mutuelle entre Alice et Eve :

$$I_{AE} = \frac{1}{2} + \frac{\Lambda[1+\varepsilon(Q)] - \Lambda[\varepsilon(Q)]}{2(1+\varepsilon(Q))} \tag{4.23}$$

$$\text{avec} \quad \varepsilon(Q) = \left(\frac{1-\sqrt{8Q(1-2Q)}}{1-4Q}\right)^2 \tag{4.24}$$

Alors que seul le protocole BB84 a été considéré dans [Lütkenhaus 1996], nous étudions dans les sous-sections suivantes les protocoles SARG04 et *six-states*.

4.4.2 six-states

Le protocole de distribution quantique de clés *six-states* est une version modifiée [Bruß 1998][Lo 2001][Bechmann-Pasquinucci 1999] de BB84 auquel une base supplémentaire a été ajoutée. Dans ce protocole, Alice peut choisir parmi les 3 bases mutuellement non biaisées (MUB an anglais pour *Mutually Unbiased Bases*) suivantes : $\{|0\rangle, |1\rangle\}$, $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ et $\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\}$.

On note habituellement ces 3 bases respectivement $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ et $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$. Ce choix d'une troisième base permet de simplifier l'étude de la sécurité de ce protocole en rendant le problème symétrique. De plus, au prix d'un taux de réjection plus important que pour BB84 (2/3 au lieu de 1/2) pendant la phase de tamisage (ou phase de *sifting*), la sécurité inconditionnelle de ce protocole a été prouvée jusqu'à un QBER plus élevé que pour BB84 : $12,6$ % au lieu de 11 %.

Pour analyser la sécurité du protocole *six-states* dans le modèle des attaques sans mémoire, on utilise le modèle intriqué équivalent de ce protocole. La méthode est identique à celle utilisée pour BB84 avec quelques adaptations au niveau de l'optimisation de l'interaction et du choix du POVM.

Optimisation de l'interaction.

Pour caractériser les états ρ_{AB} à considérer pour le protocole *six-states*, on reprend le résultat obtenu pour BB84 (et qui s'applique aussi au protocole *six-states* [Renner 2005a]) sur la forme particulière de ρ_{AB} :

$$\rho_{AB} = \alpha \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \beta \left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \gamma \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \delta \left|\Psi^-\right\rangle\left\langle\Psi^-\right| \quad \text{avec} \quad \alpha+\beta+\gamma+\delta = 1, \tag{4.25}$$

où $|\Phi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$ et $|\Psi^\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$ sont les états de Bell.

En plus de la condition de normalisation $\operatorname{Tr}\rho_{AB} = 1$, l'estimation du QBER effectuée par Alice et Bob pendant la phase de réconciliation du protocole ajoute

des contraintes sur les coefficients de ρ_{AB}. Ainsi, si on note respectivement Q_0, Q_1 et Q_2 les QBER mesurés par Alice et Bob dans les bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ et $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$ alors on obtient les relations

$$\begin{aligned} Q_0 &= \langle 01| \rho_{AB} |01\rangle + \langle 10| \rho_{AB} |10\rangle = \gamma + \delta, && (4.26)\\ Q_1 &= \langle +-| \rho_{AB} |+-\rangle + \langle -+| \rho_{AB} |-+\rangle = \beta + \delta, && (4.27)\\ Q_2 &= \langle \circlearrowleft\circlearrowleft| \rho_{AB} |\circlearrowleft\circlearrowright\rangle + \langle \circlearrowright\circlearrowleft| \rho_{AB} |\circlearrowright\circlearrowleft\rangle = \beta + \gamma. && (4.28) \end{aligned}$$

Si les QBER mesurés sur les 3 bases sont différents, cela est un signe pour Alice et Bob que le canal quantique a pu être manipulé par un attaquant. Dans ce cas, ils peuvent soit choisir d'abandonner la session du protocole et repartir de zéro soit choisir $Q = \max(Q_0, Q_1, Q_2)$ comme valeur de QBER pour le reste de la réconciliation. Dans les deux cas, Eve a alors tout intérêt à choisir une attaque pour laquelle on a $Q_0 = Q_1 = Q_2 = Q$.

Avec ces deux contraintes supplémentaires, l'état ρ_{AB} ne dépend plus que de $Q \in [0, 1/2]$ avec la relation

$$\begin{aligned} \rho_{AB} &= (1 - \frac{3Q}{2}) \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{Q}{2} \left|\Phi^-\right\rangle\left\langle\Phi^-\right| && (4.29)\\ &\quad + \frac{Q}{2} \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \frac{Q}{2} \left|\Psi^-\right\rangle\left\langle\Psi^-\right|. && (4.30) \end{aligned}$$

Pour mesurer la quantité d'information accessible à l'espionne dans ce modèle on utilise le fait que toute l'information est contenue dans une purification $|\psi\rangle\langle\psi|_{ABE}$ de ρ_{AB}. Eve est en possession de la partie ρ_E de cette purification avec

$$\rho_E = \mathrm{Tr}_{AB} |\psi\rangle\langle\psi|_{ABE}. \tag{4.31}$$

À partir de 4.29 il est facile de trouver une purification de ρ_{AB}. En effet, on voit que

$$\begin{aligned} |\psi\rangle_{ABE} &= \sqrt{1 - \frac{3Q}{2}} \left|\Phi^+\right\rangle_{AB} \left|\Phi^+\right\rangle_E + \sqrt{\frac{Q}{2}} \left|\Phi^-\right\rangle_{AB} \left|\Phi^-\right\rangle_E \\ &\quad + \sqrt{\frac{Q}{2}} \left|\Psi^+\right\rangle_{AB} \left|\Psi^+\right\rangle_E \qquad (4.32)\\ &\quad + \sqrt{\frac{Q}{2}} \left|\Psi^-\right\rangle_{AB} \left|\Psi^-\right\rangle_E. \end{aligned}$$

vérifie bien l'équation $\mathrm{Tr}_E |\psi\rangle\langle\psi|_{ABE} = \rho_{AB}$ et est donc bien une purification de ρ_{AB}.

À partir de cette purification, il est possible de calculer l'état quantique dont dispose Eve après l'interaction avec le qubit d'Alice. Ainsi, lorsqu'Alice mesure son

état dans la base b et obtient le résultat x l'état quantique d'Eve que l'on note ρ_E^{xb} s'écrit après normalisation

$$\rho_E^{xb} = \frac{\mathrm{Tr}_{AB}[|x_b\rangle\langle x_b| \otimes \mathbb{I}_B \otimes \mathbb{I}_E . \rho_{ABE}]}{\mathrm{Tr}[|x_b\rangle\langle x_b| \otimes \mathbb{I}_B \otimes \mathbb{I}_E . \rho_{ABE}]} \tag{4.33}$$

où $\rho_{ABE} = |\psi\rangle\langle\psi|_{ABE}$ est une purification de ρ_{AB}.

L'état quantique accessible à Eve après interaction avec le qubit d'Alice est donc paramétré par le seul QBER sur le canal Alice/Bob noté $Q \in [0, 1/2]$.

Optimisation de la mesure.

Après son action sur le qubit d'Alice, Eve se retrouve en possession de l'état quantique ρ_E^{xb} et doit immédiatement mesurer cet état avec un POVM qui maximise ses chances d'obtenir la valeur du bit x choisi par Alice sachant que la valeur du bit b (choix de la base utilisée par Alice) sera révélée par la suite une fois la mesure effectuée.

Dans le cas du protocole *six-states*, Eve choisit un POVM à 8 éléments qu'on peut noter $\{M_{x_0x_1x_2}\}_{x_0x_1x_2\in\{0,1\}^3}$. Pour chaque mesure, Eve obtient 3 bits d'information x_0, x_1 et x_2 et attend la révélation du choix de base $b \in \{0, 1, 2\}$ pour décider de conserver le bit x_b correspondant. Cette stratégie permet d'utiliser au mieux l'information post-mesure.

Pour que $\{M_{x_0x_1x_2}\}_{x_0x_1x_2\in\{0,1\}^3}$ forme un POVM, certaines propriétés doivent être vérifiées :

- les matrices M_i sont des opérateurs hermitiens semi-définis positifs ($M_i \geq 0$),
- $\sum_i M_i = \mathbb{I}$.

Une fois ces conditions vérifiées, on peut calculer les probabilités d'obtenir un certains résultat k lorsqu'Eve mesure l'état ρ_E^{xb} dans ce POVM :

$$p(K = k|X = x, B = b) = Tr(M_k \rho_E^{xb}). \tag{4.34}$$

Calcul de l'information mutuelle.

Après la phase de réconciliation, Eve est en possession de l'information B de la base utilisée par Alice et du résultat K de sa mesure sur son système auxiliaire. L'information mutuelle $I(X : KB)$ peut donc s'écrire

$$\begin{aligned} I(X:KB) &= H(X) + H(KB) - H(XKB) \\ &= 1 + H(K|B) + H(B) - H(K|XB) - H(XB) \\ &= H(K|B) - H(K|XB) \end{aligned} \tag{4.35}$$

où le passage de la première à la deuxième ligne s'obtient par la définition de l'entropie conditionnelle et le passage de la deuxième à la troisième ligne s'obtient en en remarquant que $H(X|B) = H(X) = 1$. En effet, X et B sont indépendants puisque choisis aléatoirement par Alice.

On peut alors calculer les entropies conditionnelles $H(K|B)$ et $H(K|XB)$ en fonctions des probabilités conditionnelles obtenues dans l'équation 4.13 :

$$\begin{aligned} H(K|XB) &= \sum_{x,b} p(X=x, B=b).H(K|X=x, B=b) \\ &= \frac{1}{8} \sum_{k,x,b} \Lambda[p(K=k|X=x, B=b)] \end{aligned} \tag{4.36}$$

$$\tag{4.37}$$

$$\text{et} \quad H(K|B) = \frac{1}{3} \sum_{k,b} \Lambda[p(K=k|B=b)] \tag{4.38}$$

Notons également ici que cette optimisation est réutilisée dans le chapitre suivant pour la preuve de sécurité du protocole *six-states* dans le modèle de la mémoire bruitée. Dans cette optique, on note $\kappa'(Q)$ le résultat de l'optimisation suivante :

$$\kappa'(Q) = \min_{strategies} H(K|XB). \tag{4.39}$$

Tracé des résultats.

Comme expliqué dans le cas de BB84, après une optimisation de l'attaque d'Eve sur l'ensemble des interactions et l'ensemble des POVMs possibles, on obtient la courbe de l'information mutuelle maximale entre Alice et Eve dans le modèle des attaques sans mémoire. Ces résultats sont tracés sur la figure 4.4.

On peut observer sur la figure 4.4 que dans le modèle d'attaque sans mémoire, Eve obtient comme prévu moins d'information que dans le cas des attaques individuelles (nécessitant l'utilisation d'une mémoire quantique) et a fortiori par rapport aux attaques collectives.

Le taux de clé en fonction du QBER sur le canal Alice/Bob est tracé en figure 4.5. On peut observer que dans le modèle de l'attaque sans mémoire, une clé peut

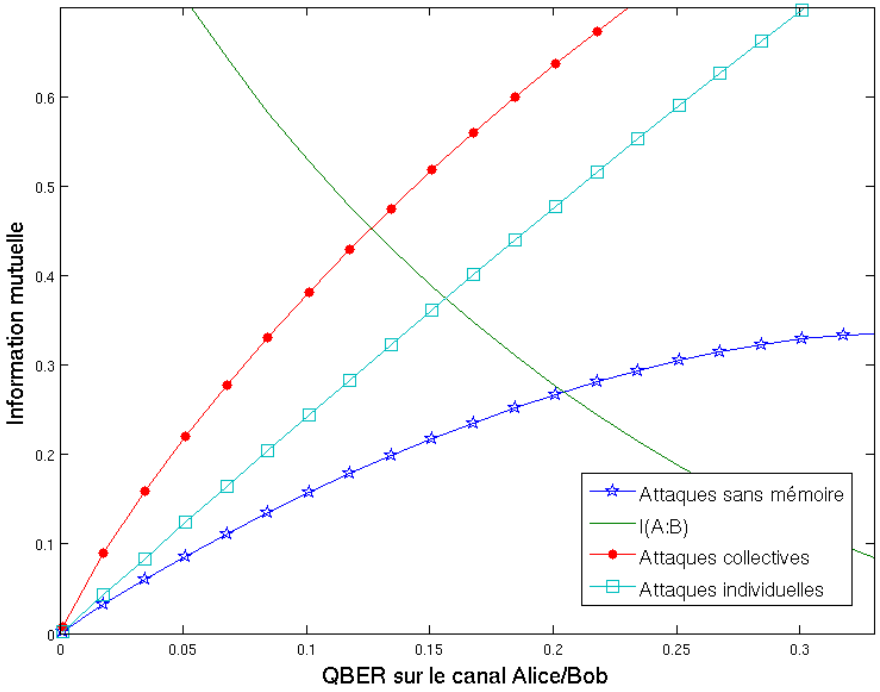


FIGURE 4.4 – Information mutuelle entre Alice et Bob et entre Alice et Eve pour le protocole *six-states* dans différents modèles de sécurité.

être générée pour un QBER inférieur à $20,4$ %, au lieu de $12,6$ % pour les attaques collectives et $15,6$ % pour les attaques individuelles.

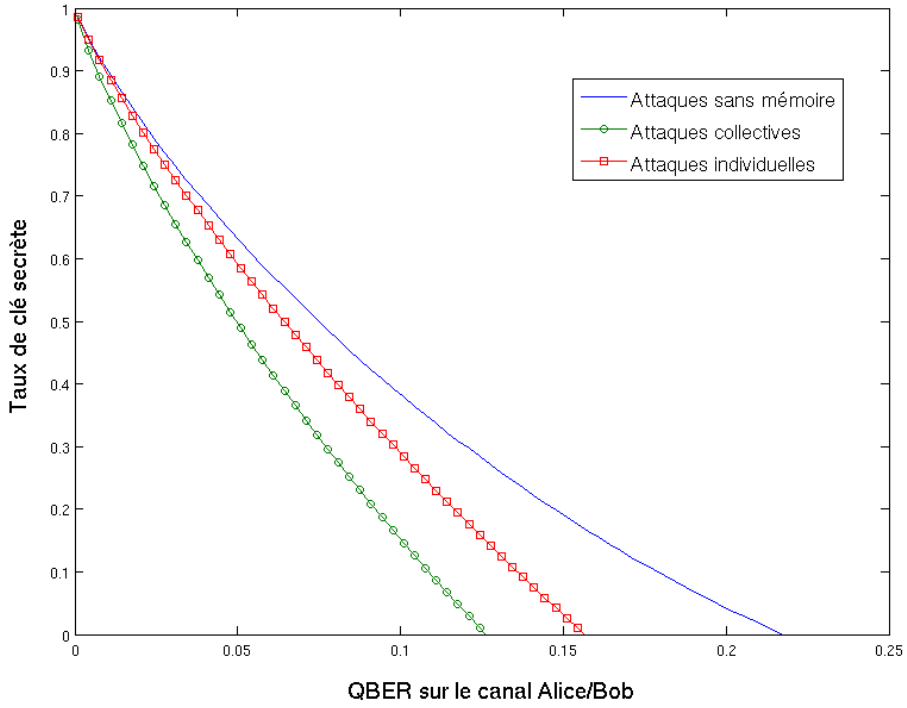


FIGURE 4.5 – Taux de clé secrète pour le protocole *six-states* dans différents modèles de sécurité.

4.4.3 SARG04

Le protocole de distribution quantique de clés SARG04 [Scarani 2004] utilise les mêmes états quantiques que le protocole BB84 mais avec un encodage différent des bits secrets. Tout comme dans BB84, Alice prépare un état $H^b |x\rangle$ dans lequel le bit secret est cette fois b au lieu de x comme dans BB84. De cette façon, les états $|0\rangle$ et $|1\rangle$ représentent le bit secret "0" et les états $|+\rangle$ et $|-\rangle$ représentent le bit secret "1".

Par exemple, on considère qu'Alice choisit le bit secret "0" et qu'elle l'encode avec l'état $|0\rangle$ sélectionné aléatoirement parmi l'ensemble $\{|0\rangle, |1\rangle\}$. Le bit sera conservé par Alice et Bob si Bob choisit de mesurer le qubit dans la base $\{|+\rangle, |-\rangle\}$. Dans ce cas Bob peut obtenir un des 2 résultats de mesure de manière équiprobable.

Pendant la phase de réconciliation, Alice va annoncer que l'état quantique envoyé faisait partie de l'ensemble $\{|0\rangle, |+\rangle\}$. Cela permet à Bob d'identifier l'état

réellement envoyé comme étant $|0\rangle$ mais ne donne pas d'information à l'espion.

Du point de vue de l'espion, l'attaque est similaire à celle pratiquée sur BB84. La principale différence se trouve dans les paramètres de la purification ρ_{ABE} du protocole intriqué équivalent. Ainsi, pour

$$\begin{aligned} \rho_{AB} &= \alpha \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \beta \left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \gamma \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \delta \left|\Psi^-\right\rangle\left\langle\Psi^-\right| \\ &\text{avec} \quad \alpha + \beta + \gamma + \delta = 1, \end{aligned} \tag{4.40}$$

on reprend les résultats de [Branciard 2005] qui nous donnent les relations

$$\begin{aligned} \alpha + \beta &= 1 - Q \\ \gamma + \delta &= Q \end{aligned} \tag{4.41}$$

de telle façon que

$$\begin{aligned} \rho_{AB} &= \alpha \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + (1 - Q - \alpha) \left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \\ &\quad (1 - \frac{3Q}{2} - \alpha) \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + (\frac{5Q}{2} - 1 + \alpha) \left|\Psi^-\right\rangle\left\langle\Psi^-\right| \end{aligned} \tag{4.42}$$

pour $\alpha \in [1 - \frac{5Q}{2}, 1 - \frac{3Q}{2}]$.

Le reste des calculs est identique à ceux déjà effectués pour BB84. Notons simplement ici que le résultat de l'optimisation est réutilisé dans le chapitre suivant pour la preuve de sécurité de SARG04 dans le modèle de la mémoire bruitée. Dans cette optique, on note $\kappa"(Q)$ le résultat de l'optimisation suivante :

$$\kappa"(Q) = \min_{strategies} H(K|XB). \tag{4.43}$$

Le résultat de la maximisation de l'information mutuelle entre Alice et Eve pour SARG04 est tracé sur la figure 4.6.

On peut observer sur la figure 4.6 que dans le modèle d'attaque sans mémoire, Eve obtient comme prévu moins d'information que dans le cas des attaques individuelles qui nécessitent une mémoire quantique.

Le taux de clé en fonction du QBER sur le canal Alice/Bob est tracé en figure 4.7. On peut observer que dans le modèle de l'attaque sans mémoire, une clé peut être générée pour un QBER inférieur à $17,5$ %, au lieu de $14,8$ % pour les attaques individuelles [Branciard 2005].

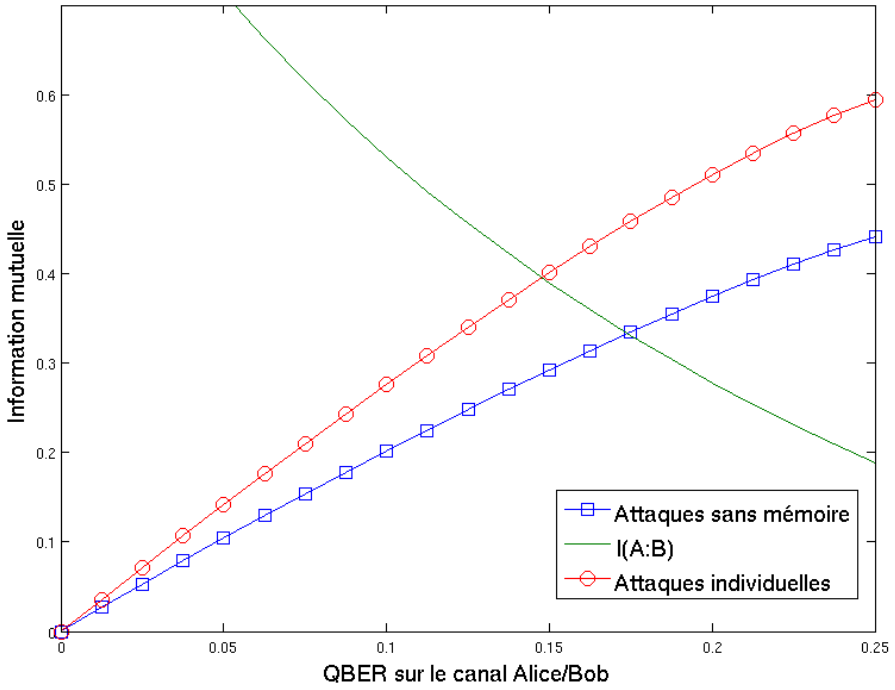


FIGURE 4.6 – Information mutuelle entre Alice et Bob et entre Alice et Eve pour SARG04 dans différents modèles de sécurité.

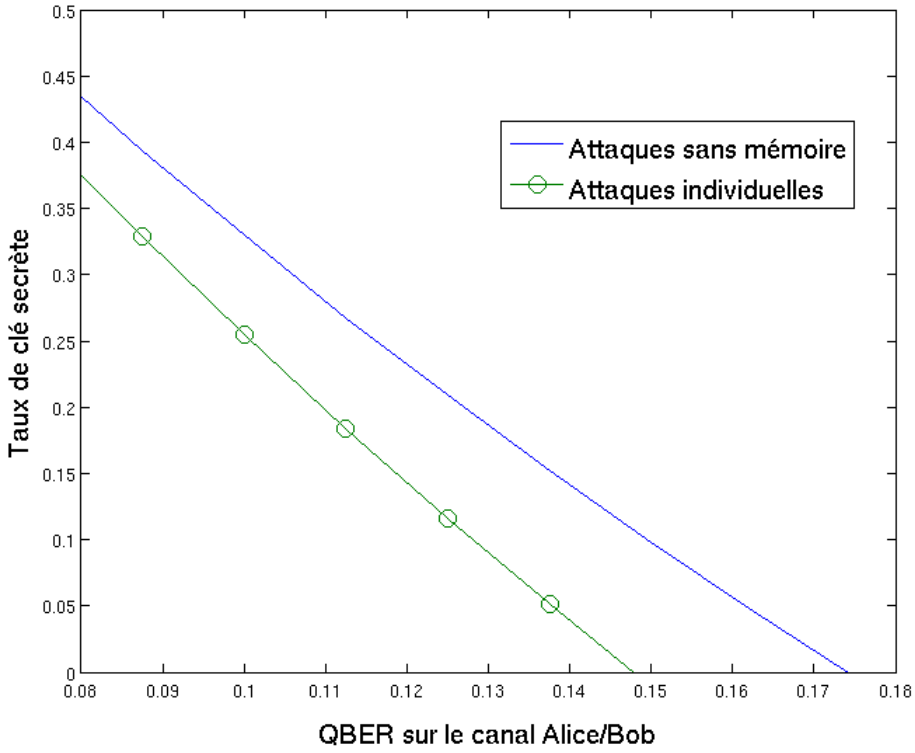


FIGURE 4.7 – Taux de clé secrète pour SARG04 dans différents modèles de sécurité.

4.4.4 Comparaison des performances des différents protocoles

Nous avons reporté dans le tableau suivant les taux d'erreur critiques au delà desquels les différents protocoles de distribution quantique de clés ne sont plus sûrs face à un adversaire n'ayant pas accès à une mémoire quantique :

Protocole	attaques individuelles	attaques sans mémoire
BB84	$14,6$ %	$15,4$ %
six-states	$15,6$ %	$20,4$ %
SARG04	$14,8$ %	$17,5$ %

En analysant les résultats résumés dans ce tableau, on remarque tout de suite que l'absence de mémoire quantique n'a pas le même impact sur l'extension du domaine de sécurité pour les trois protocoles de distribution quantique de clés étudiés. En effet, alors que pour BB84 et dans une moindre mesure SARG04 les attaques optimales sans mémoire ne sont pas beaucoup moins bonnes que les attaques individuelles, pour le protocole *six-states* l'utilisation ou non d'une mémoire quantique a un impact significatif sur le QBER critique.

Dans le cas où l'espion a une mémoire quantique et peut donc attendre la révélation des bases pour faire sa mesure, le fait qu'il y ait deux bases pour BB84 et trois pour *six-states* a moins d'impact que dans le cas où il n'a pas de mémoire quantique et doit donc mesurer immédiatement ses états quantiques en ayant une incertitude sur le choix de la base choisie par Alice (incertitude plus grande dans le cas de *six-states* en raison du nombre de bases possibles). Dans le premier cas, quel que soit le nombre de base l'espion en a connaissance au moment de la mesure et peut donc optimiser de la même façon sa mesure pour BB84 ou *six-states*. Dans le deuxième cas, lorsque l'espion n'a pas accès à une mémoire quantique sa mesure doit être un compromis entre les deux bases possibles pour BB84 et trois bases possibles pour *six-states*, d'où l'augmentation plus importante du domaine de sécurité dans ce dernier cas.

Chapitre 5

Sécurité des systèmes de distribution quantique de clés dans le modèle de la mémoire bruitée

Sommaire

Dans ce chapitre, nous allons présenter nos résultats de recherche sur la sécurité des protocoles de distribution quantique de clés lorsque l'adversaire est limité par le bruit de sa mémoire. Dans ce modèle réaliste, l'adversaire peut effectuer toutes les attaques permises par la mécanique quantique mais doit se résoudre à stocker ses états quantiques dans une mémoire quantique bruitée lorsqu'il souhaite mesurer ces états ultérieurement.

Dans une première section introductive, nous présenterons le modèle de mémoire quantique utilisé ainsi que le modèle d'attaque que nous allons considérer. Dans une deuxième section, nous présenterons des résultats obtenus sur des modèles d'attaques simplifiés qui permettent de mieux comprendre le fonctionnement des attaques. Nous détaillerons ensuite les nouvelles preuves de sécurité pour BB84 [Bennett 1984], six-states [Bruß 1998] et SARG04 [Scarani 2004] contre un adversaire limité par le bruit de sa mémoire quantique. Enfin la dernière section sera consacrée à une comparaison des performances de ces 3 protocoles dans le modèle de la mémoire quantique bruitée.

5.1 Introduction

Au cœur de notre modèle d'espion se trouve la mémoire quantique bruitée. Nous allons présenter ici le modèle de mémoire quantique que nous utiliserons dans les preuves de sécurité des sections suivantes. Nous exposerons dans un deuxième temps les idées générales du modèle d'attaque considéré.

5.1.1 État de l'art sur les mémoires quantiques

L'objectif est ici de dresser un rapide état de l'art en matière de mémoires quantiques en évoquant leur intérêt en information quantique, les différentes implémentations et leurs performances. Cet exposé restant succinct, nous dirigeons le lecteur vers [Simon 2010, Lauritzen 2010] pour plus d'informations.

Mémoire quantique : composant clé d'un grand nombre d'applications en information quantique.

La recherche sur les mémoires quantiques a été stimulée par le grand nombre d'applications de cette technologie dans de nombreux domaines de l'information quantique. Parmi ces applications, on peut citer notamment l'ordinateur quantique ou le répéteur quantique.

Cette dernière application est intimement liée à la distribution quantique de clés puisque le répéteur quantique a été proposé comme un moyen de prolonger la distance accessibles aux protocoles de distribution quantique de clés dont la portée limitée est aujourd'hui un des inconvénients majeurs. En effet, les pertes sur le canal quantique habituellement compensés par des amplificateurs optiques dans les systèmes de communication optique à longue distance ne sont pas utilisables dans le cas de la distribution quantique de clés en raison de la perte de cohérence associée à toute opération d'amplification comme le théorème de non clonage nous l'assure.

Le répéteur quantique permet de contourner cette limitation fondamentale. Le principe est de diviser la distance en plusieurs segments de longueur compatible avec les performances des protocoles de distribution quantique de clés et de créer

des paires intriquées sur chacun de ces segments de manière indépendantes. À leur création, ces paires sont stockées dans des mémoires quantiques le temps de la création de paires intriquées sur l'ensemble des segments. Il est alors possible à l'aide d'une opération appelée transfert d'intrication d'obtenir une paire intriquée entre les deux extrémités de la chaînes. Un protocole tel que BBM92 [Bennett 1992b] peut ensuite utiliser cette ressource d'intrication pour générer une clé secrète à longue distance.

Paramètres caractérisant la qualité d'une mémoire.

La qualité d'une mémoire quantique est définie par de nombreux paramètres. Nous allons ici nous intéresser aux trois principaux : l'efficacité, la fidélité et le temps de stockage. Ces paramètres ne sont pas forcément indépendants. Par exemple il est clair que le temps de stockage et la fidélité sont en concurrence : on peut choisir un temps de stockage plus long pour une technologie au prix d'une baisse de la fidélité ou le contraire.

L'efficacité est la capacité de la mémoire à restituer l'information après son stockage. Par exemple dans le cas d'une mémoire pour photons uniques, elle est définie comme la probabilité qu'un photon soit émis après la période de stockage conditionnée à la probabilité qu'un photon ait été effectivement stocké.

La fidélité représente la quantité de dégradation introduite par la mémoire sur l'état quantique stocké. Une fidélité proche de l'unité signifie que la mémoire a introduit très peu de bruit et vice versa. La définition mathématique utilisée en pratique varie selon les sources et nous ne nous attarderons pas dessus.

Le temps de stockage représente la durée au bout de laquelle la mémoire est censée retourner l'état quantique qui y a été stocké.

D'autres critères peuvent être considérés en fonction des applications spécifiques de la mémoire quantique, on peut par exemple différencier la longueur d'onde de fonctionnement de la mémoire ou la bande passante par exemple. En fonction des caractéristiques souhaitées pour une utilisation particulière de la mémoire quantique, différentes technologies pourront être utilisées.

Les différents types de mémoire quantique.

Il existe de nombreuses façons d'implémenter une mémoire quantique, chaque méthode ayant ses avantages et ses inconvénients. Nous avons choisi d'illustrer notre propos avec deux exemples de mémoire quantique.

Une première méthode triviale pour obtenir une mémoire quantique est l'utilisation d'une ligne à retard fibrée ou en espace libre qui permet un stockage de l'information pendant toute la durée de la transmission dans le canal considéré. Dans ce cas la durée de stockage est limitée par le rapport de la longueur de la ligne à retard à la vitesse de propagation de la lumière dans le milieu. Par exemple pour une fibre optique d'environ 60 km dont les pertes sont de 90 % on peut espérer obtenir une mémoire avec une efficacité de 10 % et une durée de stockage de 250 μs. Au delà des performances médiocres de cette méthode, l'inconvénient majeur est que la durée de stockage est fixée par la longueur de la ligne à retard. Cette méthode représente en quelque sorte le niveau minimum de qualité espéré dans une mémoire quantique.

Une deuxième méthode couramment employée met en oeuvre la transparence électromagnétiquement induite (appelé EIT en anglais) [Boller 1991] [Kasapi 1995] [Budker 1999]. L'EIT est un phénomène d'optique non linéaire observée dans certains matériaux présentant une structure particulière de niveaux d'énergie. L'idée est d'utiliser des champs magnétiques pour manipuler la vitesse de groupe de l'onde électromagnétique qui traverse ce milieu et la faire tendre vers 0. Ainsi la lumière très fortement ralentie voire arrêtée peut être récupérée à la demande quelques instants plus tard.

Cette propriété physique est exploitée dans les mémoires quantiques à base de peigne de fréquence atomique [Afzelius 2009] et permet d'atteindre une efficacité de 34 %, une fidélité de 96 % et un temps de stockage de l'ordre de 15 μs. Ces performances sont du même ordre de grandeur pour la plupart des autres implémentations de mémoire quantique.

Au mieux, des temps de stockage de l'ordre de la dizaine de millisecondes ont été observés : on peut citer l'exemple de [Julsgaard 2004] basé sur des vapeurs atomiques qui a permis d'atteindre une fidélité de 70 % et un temps de stockage de 4 ms.

L'état actuel de la recherche sur les mémoires quantiques nous permet donc d'affirmer que supposer qu'un adversaire ne peut avoir accès qu'à une quantité limitée de mémoire imparfaite est une hypothèse réaliste. Comme nous l'expliquons dans le paragraphe suivant, il est en effet facile d'imposer à l'adversaire un temps d'attente suffisamment long pour que la mémoire quantique disponible ait une fidélité faible.

Utilisation d'une mémoire quantique par un espion.

Dans le cadre d'un protocole de distribution quantique de clés, le temps d'attente est imposé à l'espion par un paramètre contrôlé par les utilisateurs légitimes. Ce paramètre est en général un délai entre la phase de distribution d'états quantiques et la phase de réconciliation pendant laquelle des informations classiques sont

échangées. Ce délai peut être choisi arbitrairement long pourvu que la latence dans l'établissement des clés ainsi générées ne soit pas problématique. Cela signifie en pratique qu'on peut supposer qu'un espion ne peut avoir accès à une mémoire quantique parfaite. Il peut au mieux avoir accès à une mémoire quantique bruitée (c'est ce qui nous intéresse dans ce chapitre) ou pas de mémoire quantique du tout, un cas que nous avons déjà étudié dans le chapitre précédent.

5.1.2 Modélisation de la mémoire de l'espion

Une mémoire quantique permet le stockage temporaire d'un état quantique décrit par un espace de Hilbert de dimension finie pendant un temps de stockage t. Les éventuelles dégradations de l'état qui peuvent intervenir pendant ce stockage peuvent être de nature diverse et aller de la conservation parfaite à la perte totale de l'information. Dans tous les cas, cette évolution peut être représentée par un canal quantique c'est à dire une application linéaire $\mathcal{N}$ dans l'espace des opérateurs densité.

De manière générale, le canal décrivant une mémoire quantique dépend du temps de stockage t. Si un état quantique est stocké dans la mémoire à l'instant $t = 0$ alors la transformation subie par cet état au bout d'un temps t est représentée par le canal $\mathcal{N}^t$. Afin de refléter les propriétés naturelles d'une mémoire quantique, on suppose que le canal initial $\mathcal{N}^0$ est égal au canal identité et surtout que le bruit dans le canal ne peut qu'augmenter avec le temps. Ainsi, un adversaire ne peut pas espérer obtenir plus d'information à la sortie du canal en attendant plus longtemps.

Compte tenu de ces hypothèses réalistes le canal représentant la mémoire quantique est entièrement déterminé par $t_{\min}$, le temps minimal de stockage imposé à l'espion par le protocole. Dans ce cas le meilleur canal est $\mathcal{N}^{t_{\min}}$ et on écrira tout simplement dans la suite de cette partie $\mathcal{N} = \mathcal{N}^{t_{\min}}$.

L'application linéaire $\mathcal{N}$ accepte en entrée des états quantiques décrits par l'espace de Hilbert d'entrée $\mathcal{S}(\mathcal{H}_{in})$ et prend ses valeurs dans l'espace de Hilbert de sortie $\mathcal{S}(\mathcal{H}_{out})$. Ainsi, on peut décrire mathématiquement la mémoire quantique de la façon suivante :

$$\begin{array}{rcl} \mathcal{N} : \mathcal{S}(\mathcal{H}_{in}) & \longrightarrow & \mathcal{S}(\mathcal{H}_{out}) \\ \rho_{in} & \longmapsto & \rho_{out} = \mathcal{N}(\rho_{in}). \end{array} \tag{5.1}$$

On rappelle que les propriétés suivantes sont vérifiées par l'application $\mathcal{N}$:

- elle est linéaire,
- elle est positive, c'est à dire $\rho_{in} \geq 0 \Rightarrow \mathcal{N}(\rho_{\text{in}}) \geq 0$,

- elle conserve la trace, c'est à dire $\mathrm{Tr}\,\mathcal{N}(\rho_{in}) = \mathrm{Tr}\,\rho_{in}$.

Dans cette description, la dimension de l'espace de Hilbert d'entrée est au moins égale au nombre de degrés de liberté du système quantique à stocker. Il serait pourtant beaucoup plus facile de manipuler des espaces de Hilbert de dimension 2 où seuls des qubits peuvent être stockés. C'est pour cette raison que nous allons maintenant transformer ce modèle de mémoire quantique afin de le simplifier.

La première étape de cette simplification est de décomposer le canal $\mathcal{N}$ en un produit tensoriel de canaux quantiques $\mathcal{M}$ agissant sur des qubits. On peut décrire ces canaux de la façon suivante :

$$\begin{array}{rcl} \mathcal{M} : \mathcal{S}(\mathbb{C}^2) & \longrightarrow & \mathcal{S}(\mathbb{C}^2) \\ \rho_{in} & \longmapsto & \rho_{out} = \mathcal{M}(\rho_{in}). \end{array} \tag{5.2}$$

Dans ce cas, le canal $\mathcal{N}$ est représenté par un produit tensoriel d'un nombre q de canaux $\mathcal{M}$:

$$\mathcal{N} = \mathcal{M}^{\otimes q} \tag{5.3}$$

Dans le contexte de la distribution quantique de clés où on assiste à l'échange de n qubits entre Alice et Bob, il sera utile dans la suite de ce chapitre d'exprimer q en tant que fraction de ce nombre de qubits échangés. Ainsi on peut définir la fraction ν décrivant la taille de la mémoire de l'espion par la relation $q = \nu n$.

Au lieu de considérer l'ensemble des canaux agissant sur les qubits, il pourra être utile par la suite de considérer l'exemple important du canal à dépolarisation. Ce canal est en effet abondamment étudié dans la littérature [King 2001, Medeiros 2008]. On se rappelle alors que le canal à dépolarisation de paramètre de bruit p noté $\mathcal{D}_p$ peut s'écrire :

$$\begin{array}{rcl} \mathcal{D}_p : \mathcal{S}(\mathbb{C}^2) & \longrightarrow & \mathcal{S}(\mathbb{C}^2) \\ \rho_{in} & \longmapsto & \rho_{out} = \frac{p\mathbb{I}}{2} + (1-p)\rho_{in} \end{array} \tag{5.4}$$

où le paramètre p peut prendre ses valeurs entre 0 et 1.

Ainsi le canal représentant la mémoire de l'espion peut s'écrire :

$$\mathcal{N} = \mathcal{D}_p^{\otimes \nu n}. \tag{5.5}$$

5.1.3 Preuve de sécurité et attaque optimale

Nous souhaitons ici définir précisément ce que nous entendons par modèle d'attaque, preuve de sécurité et attaque optimale.

Un **modèle d'attaque** définit l'ensemble des contraintes imposées à l'espion dans le but de faciliter l'analyse de la sécurité du protocole. Le choix du bon modèle d'attaque est un compromis entre une généralité suffisante pour se rapprocher des contraintes réelles d'un attaquant et une complexité suffisamment faible pour permettre l'analyse de la sécurité du protocole.

Pour décrire une **attaque optimale**, on commence par fabriquer un modèle d'attaque dans lequel la puissance de l'espion est suffisamment limitée pour permettre une paramétrisation complète de son action. Il est alors possible d'optimiser l'attaque de l'espion sur l'ensemble de ces paramètres de façon à maximiser l'information mutuelle entre l'espion et les participants honnêtes. Le résultat de cette optimisation est une description explicite de la meilleure attaque du modèle considéré, ce que nous appelons l'attaque optimale dans ce modèle.

En faisant ainsi on prouve explicitement qu'un espion a la possibilité d'obtenir une certaine quantité d'information sur la clé grâce à une méthode démontrée. Sous réserve d'une bonne paramétrisation du problème, l'optimalité de l'attaque nous assure qu'un espion soumis aux contraintes du modèle ne peut pas obtenir plus d'information avec une autre attaque.

Comme nous l'avons déjà évoqué, il est impossible de caractériser complètement les attaques les plus générales autorisées par la mécanique quantique, les attaques cohérentes. Cette technique n'est donc applicable que pour des modèles de sécurité où la puissance de l'espion est limitée : c'est par exemple le cas du modèle des attaques individuelles pour le protocole BB84 où l'action de l'espion peut être réduite à un nombre raisonnable de paramètres.

Une **preuve de sécurité** donne l'assurance de la sécurité d'un protocole contre un adversaire soumis aux contraintes du modèle de sécurité considéré (voire sans contraintes dans le cas du modèle des attaques cohérentes). On parle de preuve de sécurité optimale lorsqu'il existe une attaque explicite qui atteint la frontière du domaine de sécurité obtenu par la preuve.

Dans les sections suivantes, nous allons commencer par construire des attaques explicites sur deux protocoles de distribution quantique de clés, BB84 et *six-states* dans un modèle de sécurité suffisamment contraignant sur l'adversaire pour pouvoir les paramétrer complètement. Par la suite nous présenterons une preuve de sécurité des trois protocoles de distribution quantique de clés dans un modèle plus général pour lequel il n'est pas possible d'exhiber explicitement une attaque.

5.2 Attaques explicites dans le modèle de la mémoire bruitée

Avant de se lancer dans la preuve de sécurité proprement dite, il est utile de s'attarder sur un modèle relativement simple d'attaque de l'espion qui permet d'introduire des outils qui seront utiles par la suite.

5.2.1 Construction explicite d'une attaque sur BB84

Cette construction explicite s'inspire de l'attaque individuelle optimale décrite dans [Gisin 2002] et d'une attaque collective optimale [Pirandola 2008] sur BB84 dans le cas d'une mémoire quantique parfaite. Ici, l'attaque naïve avec mémoire bruitée consiste à reproduire les mêmes interactions et mesures que dans le cas idéal mais en utilisant une mémoire bruitée. La faiblesse de ce modèle est de considérer que l'espion utilise sa mémoire quel que soit son bruit sans possibilité de se rabattre sur une autre méthode en cas de bruit trop important. Cette faiblesse est aussi ce qui permet de paramétriser facilement l'ensemble des attaques possibles sous cette contrainte.

On imagine bien que lorsque le bruit de la mémoire tend vers 1 c'est à dire quand la mémoire devient complètement bruitée cette méthode ne permettra pas à l'espion d'obtenir de l'information sur la clé alors qu'une attaque ne nécessitant pas de mémoire aurait été plus efficace dans ce cas. Cette méthode réduit donc arbitrairement la puissance de l'espion mais permettra tout de même d'introduire des outils utiles pour la suite et de faciliter la compréhension de la preuve.

Limitation de la puissance de l'espion.

On considère un protocole de distribution quantique de clés entre Alice et Bob. Au cours de la phase quantique, Alice choisit d'encoder un message sur un état quantique et le transmet à Bob qui effectue une mesure sur cet état et stocke le résultat dans une mémoire classique.

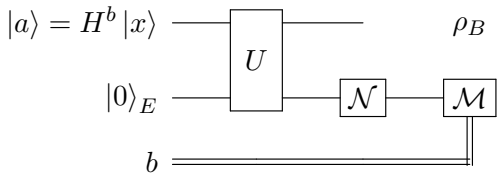
Pendant cette phase quantique, l'espionne Eve effectue les actions suivantes :

1. Elle réalise une opération unitaire U de son choix entre le qubit envoyé par Alice et un système auxiliaire qu'elle conserve dans son laboratoire.

2. Elle stocke ce système auxiliaire dans une mémoire quantique bruitée.

3. Pendant la phase de réconciliation lorsque l'information de la base utilisée par Alice est annoncée elle effectue une mesure sur sa mémoire quantique pour extraire le maximum d'information sur le bit secret.

Plus précisément, on considère qu'Alice et Bob utilisent le protocole BB84. Ainsi, Alice choisit un bit secret x et une base b qui prennent leurs valeurs dans l'ensemble $\{0,1\}$ et fabrique l'état $|a\rangle = H^b |x\rangle$ (où H représente la transformation de Hadamard) avant de l'envoyer à Bob. Si on considère que le système auxiliaire utilisé par Eve se trouve initialement dans l'état $|0\rangle_E$ et que la mémoire quantique d'Eve est représentée par le canal $\mathcal{N}$ alors on peut décrire l'ensemble de l'attaque d'Eve par le circuit quantique suivant :



(5.6)

FIGURE 5.1 – Circuit quantique représentant une attaque simple avec mémoire quantique bruitée.

On note $\mathcal{H}_A$, $\mathcal{H}_B$ et $\mathcal{H}_E$ les espaces de Hilbert d'Alice, Bob et Eve. Ainsi, l'opération unitaire U utilisée par Eve pour intriquer son système auxiliaire au qubit d'Alice est décrit par :

$$U : \mathcal{H}_A \otimes \mathcal{H}_E \longrightarrow \mathcal{H}_B \otimes \mathcal{H}_E \tag{5.7}$$

$$|a\rangle \otimes |0\rangle_E \longmapsto U(|a\rangle \otimes |0\rangle_E). \tag{5.8}$$

On considère que l'espace de Hilbert d'Eve $\mathcal{H}_E$ est de dimension 4, en effet elle ne peut pas gagner plus d'information avec un espace de Hilbert plus grand [Gisin 2002]. On calcule alors l'état de sortie $|\phi\rangle_{BE}$ en utilisant sa décomposition de Schmidt :

$$|\phi\rangle_{BE} = U\left(|a\rangle \otimes |0\rangle_E\right) = |a\rangle |F_a\rangle + |a \oplus 1\rangle |Q_a\rangle , \tag{5.9}$$

où a prend ses valeurs dans l'ensemble $\{0,1,+,\times\}$ et où $a \oplus 1 = \{1,0,\times,+\}$. De plus $\{|a\rangle , |a \oplus 1\rangle\}$ est une base orthonormale de $\mathcal{H}_A$ et $|F_a\rangle , |Q_a\rangle \in \mathcal{H}_E$.

En suivant la même méthode que [Pirandola 2008] et [Gisin 2002] on suppose que l'attaque considérée est symétrique ce qui nous permet d'écrire les relations suivantes :

$$\forall a \in \{0,1,+,\times\}, \quad \langle F_a|F_a\rangle = F, \tag{5.10}$$
$$\langle Q_a|Q_a\rangle = Q = 1-F, \tag{5.11}$$
$$\langle F_a|Q_a\rangle = 0. \tag{5.12}$$

Ainsi les canaux créés entre Alice et Bob noté $\mathcal{E}_B^U$ et Alice et Eve noté $\mathcal{E}_E^U$ peuvent s'écrire :

$$\rho_B(a) = \mathcal{E}_B^U(|a\rangle\langle a|) = tr_E\left(U|a\rangle|0\rangle_E\langle 0|_E\langle a^*|U^\dagger\right) \tag{5.13}$$
$$= F|a\rangle\langle a| + Q|a\oplus 1\rangle\langle a\oplus 1| \tag{5.14}$$
$$\rho_E(a) = \mathcal{E}_E^U(|a\rangle\langle a|) = tr_A\left(U|a\rangle|0\rangle_E\langle 0|_E\langle a^*|U^\dagger\right) \tag{5.15}$$
$$= |F_a\rangle\langle F_a| + |Q_a\rangle\langle Q_a| \tag{5.16}$$
$$= F|f_a\rangle\langle f_a| + Q|q_a\rangle\langle q_a| \tag{5.17}$$

où $|f_a\rangle = 1/\sqrt{F}|F_a\rangle$ et $|q_a\rangle = 1/\sqrt{Q}|Q_a\rangle$. Les normes F et Q représentent respectivement la fidélité et le QBER sur le canal Alice/Bob.

L'état $\rho_E(a)$ obtenu par Eve après l'interaction doit être stocké dans une mémoire quantique. Nous allons ici considérer que la mémoire quantique est représentée par un canal à dépolarisation de paramètre de bruit p. Ainsi, l'état quantique en sortie de mémoire $\tilde{\rho}_E(a)$ peut s'écrire :

$$\tilde{\rho_E}(a) = \mathcal{D}_p(\rho_E(a)) = \frac{p\mathbb{I}}{4} + (1-p)\rho_E(a). \tag{5.18}$$

Une fois l'information de la base obtenue, l'objectif d'Eve est de pouvoir distinguer les deux états possibles $\tilde{\rho_E}(a)$ et $\tilde{\rho_E}(a\oplus 1)$ pour $a \in \{0,+\}$ en fonction de la base utilisée par Alice. La façon optimale d'effectuer cette opération est connue depuis longtemps sous la forme du théorème de Helstrom [Helstrom 1969] :

Théorème de Helstrom : *Pour deux états quantiques ρ_0 et ρ_1 obtenus avec les probabilité q et $1-q$ respectivement, la probabilité de deviner correctement lequel des*

deux états a été mesuré est au maximum

$$p_{dev.} = \frac{1}{2}[1 + \|q\rho_0 - (1-q)\rho_1\|_1]. \tag{5.19}$$

De plus la mesure qui permet d'atteindre $p_{dev.}$ est donnée par les éléments M_0 et $M_1 = \mathbb{I} - M_0$, où M_0 est le projecteur sur l'espace propre associé à la valeur propre positive de $q\rho_0 - (1-q)\rho_1$.

Si on applique ce théorème à notre cas, la probabilité qu'Eve obtienne le bon résultat en utilisant cette mesure optimale est :

$$p_{\text{dev.}} = \frac{1}{2}\left[1 + \left\| \frac{\tilde{\rho_E}(a) - \tilde{\rho_E}(a \oplus 1)}{2} \right\|_1 \right]. \tag{5.20}$$

Afin de pouvoir calculer cette probabilité, il est nécessaire de développer le calcul de $\rho_E(a)$. En utilisant l'ensemble des contraintes imposées par les équations 5.10, 5.11 et 5.12 on peut réduire le nombre de paramètres du problème en suivant la méthode employée par [Gisin 2002]. Ainsi, on introduit deux nouvelles variables x et y prenant leur valeur dans $[0, 2\pi]$ et définies par les relations

$$\langle F_a | F_{a\oplus 1} \rangle = F \cos x, \tag{5.21}$$
$$\langle Q_a | Q_{a\oplus 1} \rangle = F \cos y \tag{5.22}$$

On peut alors facilement vérifier que les choix suivants permettent de respecter toutes les conditions imposées jusqu'à maintenant :

$$|F_a\rangle = \begin{pmatrix} \sqrt{F} \\ 0 \\ 0 \\ 0 \end{pmatrix}, |Q_a\rangle = \begin{pmatrix} 0 \\ \sqrt{Q} \\ 0 \\ 0 \end{pmatrix} \tag{5.23}$$

$$|F_{a\oplus 1}\rangle = \begin{pmatrix} \sqrt{F}\cos x \\ 0 \\ 0 \\ \sqrt{F}\sin x \end{pmatrix}, |Q_{a\oplus 1}\rangle = \begin{pmatrix} 0 \\ \sqrt{Q}\cos y \\ \sqrt{Q}\sin y \\ 0 \end{pmatrix} \tag{5.24}$$

On peut alors calculer les valeurs de $\rho_E(a)$ et $\rho_E(a \oplus 1)$ pour $a \in \{0, +\}$:

$$\rho_E(a) = |F_a\rangle \langle F_a| + |Q_a\rangle \langle Q_a| \tag{5.25}$$
$$\rho_E(a \oplus 1) = |F_{a\oplus 1}\rangle \langle F_{a\oplus 1}| + |Q_{a\oplus 1}\rangle \langle Q_{a\oplus 1}|. \tag{5.26}$$

En reprenant la formule

$$p_{\text{dev.}} = \frac{1}{2}\left[1 + \left\| \frac{\tilde{\rho_E}(a) - \tilde{\rho_E}(a \oplus 1)}{2} \right\|_1\right]. \tag{5.27}$$

où $\|\sigma\|_1 = \text{Tr}\sqrt{\sigma\sigma^\dagger}$ et en optimisant les valeurs de x et de y afin de maximiser p_{dev} on obtient le résultat suivant :

$$p_{\text{dev.}} = \frac{1}{2} + (1-p)\sqrt{Q(1-Q)}. \tag{5.28}$$

Le graphe de la fonction $p_{\text{dev.}}(Q)$ pour différentes valeurs de bruit p est tracé en figure 5.2.

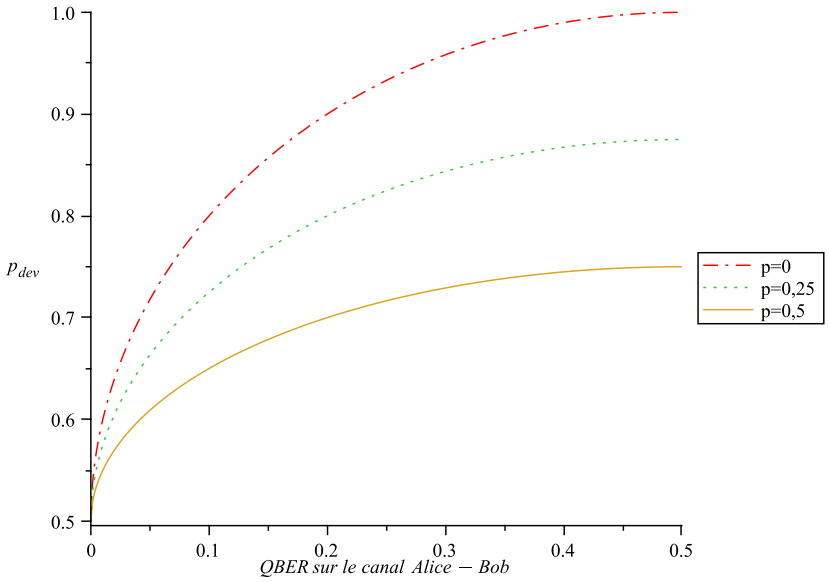


FIGURE 5.2 – Probabilité de réussite de l'attaque d'Eve en fonction du QBER sur le canal Alice/Bob pour différentes valeurs de bruit dans la mémoire pour le protocole BB84.

L'information mutuelle entre Alice et Bob s'obtient facilement par la relation :

$$I_{AB} = 1 - h(Q). \tag{5.29}$$

Quant à l'information mutuelle entre Alice et Eve on l'obtient grâce à la probabilité de succès $p_{\text{dev.}}$ pour finalement avoir :

$$I_{AE} = 1 - h(\frac{1}{2} + (1-p)\sqrt{Q(1-Q)}). \tag{5.30}$$

Le taux de clé sécrète R s'obtient alors par la relation $R = I_{AB} - I_{AE}$. Le graphe de cette fonction est dessiné en figure 5.3.

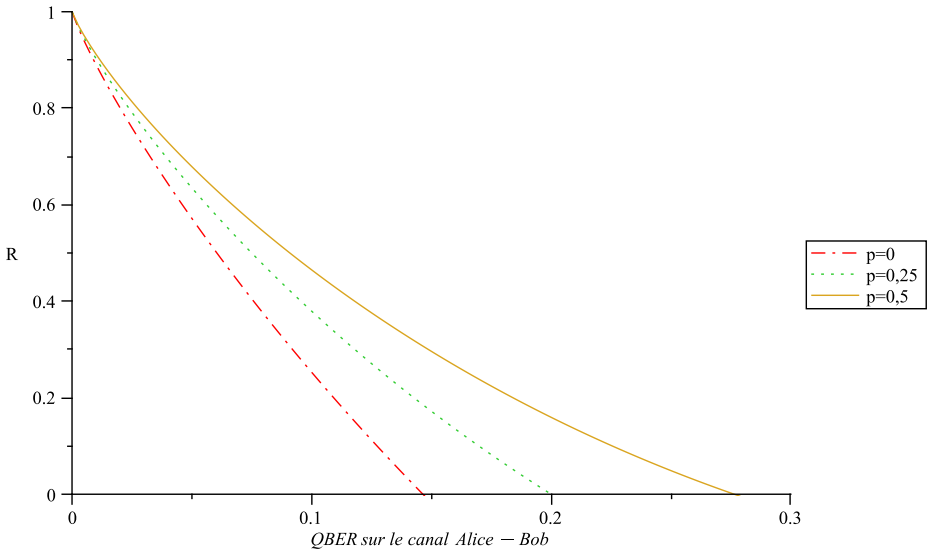


FIGURE 5.3 – Taux de clé secrète R en fonction du QBER sur le canal Alice/Bob pour différentes valeurs de bruit dans la mémoire pour le protocole BB84.

On peut remarquer que dans le cas limite d'une mémoire sans bruit ($p = 0$) ce modèle d'attaque correspond à l'attaque individuelle optimale sur BB84 [Gisin 2002] et que dans ce cas le taux de clé devient nul pour $Q = 14,6$ %. Comme on pouvait s'y attendre l'attaque est moins efficace lorsque le bruit dans la mémoire quantique augmente.

On mesure également l'ampleur de la contrainte imposée à l'espion : en l'obligeant à utiliser sa mémoire quantique même lorsque le bruit devient important, on le prive de la possibilité de se rabattre sur une attaque plus efficace ne nécessitant pas de mémoire quantique. On rappelle ici le résultat obtenu dans le chapitre précédent sur les attaques optimales sans mémoire sur BB84 : il existe une attaque sans mémoire quantique qui annule le taux de clé secrète dès que le taux d'erreur sur le canal quantique est supérieur à $15,4$ %. L'attaque avec mémoire quantique bruitée que nous venons de décrire est meilleure que cette attaque sans mémoire lorsque

le bruit p dans la mémoire est inférieur à 4 % c'est à dire lorsque la mémoire est quasiment parfaite.

Dans la sous-section suivante, nous appliquons la même méthode au protocole *six-states*.

5.2.2 Attaque explicite simple sur le protocole *six-states*

Le protocole *six-states* peut se voir comme une extension de BB84 auquel on ajoute une troisième base. Ainsi, Alice peut choisir d'encoder son bit secret sur une nouvelle paire d'état qu'on note $\{|\circlearrowright\rangle, |\circlearrowleft\rangle\}$ et qui est définie de la manière suivante :

$$\{|\circlearrowright\rangle, |\circlearrowleft\rangle\} = \{\frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}\} \tag{5.31}$$

Comme dans le cas de BB84, on peut décomposer l'état d'Eve après l'interaction de la façon suivante :

$$\forall a \in \{0, +, \circlearrowright\} \qquad \rho_E(a) = |F_a\rangle\langle F_a| + |Q_a\rangle\langle Q_a| \tag{5.32}$$

$$\rho_E(a \oplus 1) = |F_{a\oplus 1}\rangle\langle F_{a\oplus 1}| + |Q_{a\oplus 1}\rangle\langle Q_{a\oplus 1}| \tag{5.33}$$

Par contre la différence avec BB84 vient du fait que le QBER sur le canal Alice-Bob est estimé sur les 3 bases. Cela impose une contrainte supplémentaire sur le choix des paramètres de l'attaque d'Eve. Plus précisément, la contrainte $\langle F_0|F_0\rangle = \langle F_+|F_+\rangle = \langle F_\circlearrowright|F_\circlearrowright\rangle$ une fois développée impose la relation

$$F = \frac{1}{2}(1 + F\cos x + Q\cos y) = \frac{1}{2}(1 + F\cos x - Q\cos y). \tag{5.34}$$

Cette condition ne peut être vérifiée que si $y = \frac{\pi}{2} \mod \pi$ et si la relation suivante est vraie :

$$\cos x = \frac{1-2Q}{1-Q}. \tag{5.35}$$

On peut alors obtenir les expressions des vecteurs $|F\rangle$ et $|Q\rangle$:

$$|F_a\rangle = \begin{pmatrix}\sqrt{F}\\0\\0\\0\end{pmatrix}, |Q_a\rangle = \begin{pmatrix}0\\\sqrt{Q}\\0\\0\end{pmatrix} \tag{5.36}$$

$$|F_{a\oplus 1}\rangle = \begin{pmatrix}\sqrt{F}\cos x\\0\\0\\\sqrt{F}\sin x\end{pmatrix}, |Q_{a\oplus 1}\rangle = \begin{pmatrix}0\\0\\\sqrt{Q}\\0\end{pmatrix} \tag{5.37}$$

En reprenant la formule

$$p_{\text{dev.}} = \frac{1}{2}\left[1 + \left\| \frac{\tilde{\rho_E}(a) - \tilde{\rho_E}(a \oplus 1)}{2} \right\|_1 \right]. \tag{5.38}$$

on obtient le résultat suivant :

$$p_{\text{dev.}} = \frac{1}{2}\left[1 + (1-p)\left(Q + \sqrt{Q(2-3Q)}\right)\right]. \tag{5.39}$$

Le graphe de la fonction $p_{\text{dev.}}(Q)$ pour différentes valeurs de bruit p est tracé en figure 5.4.

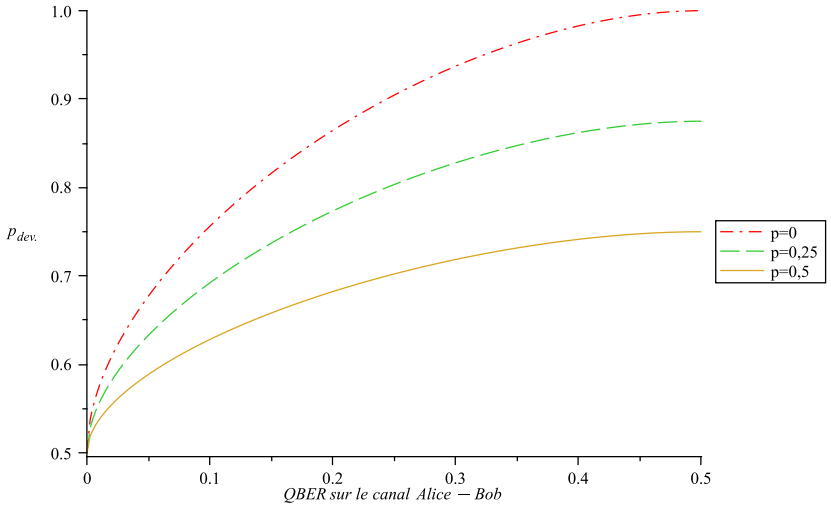


FIGURE 5.4 – Probabilité de réussite de l'attaque d'Eve en fonction du QBER sur le canal Alice/Bob pour différentes valeurs de bruit dans la mémoire sur le protocole *six-states*.

Le taux de clé sécrète R s'obtient alors par la relation $R = I_{AB} - I_{AE}$. En développant on obtient :

$$R = h(\frac{1}{2} + \frac{1-p}{2}\left(Q + \sqrt{Q(2-3Q)}\right)) - h(Q). \tag{5.40}$$

Le graphe de cette fonction est dessiné en figure 5.5.

Dans le cas limite d'une mémoire sans bruit ($p = 0$) ce modèle d'attaque correspond à l'attaque individuelle sur le protocole *six-states* décrite dans [Bruß 1998]. Comme pour BB84, l'attaque est moins efficace lorsque le bruit dans la mémoire

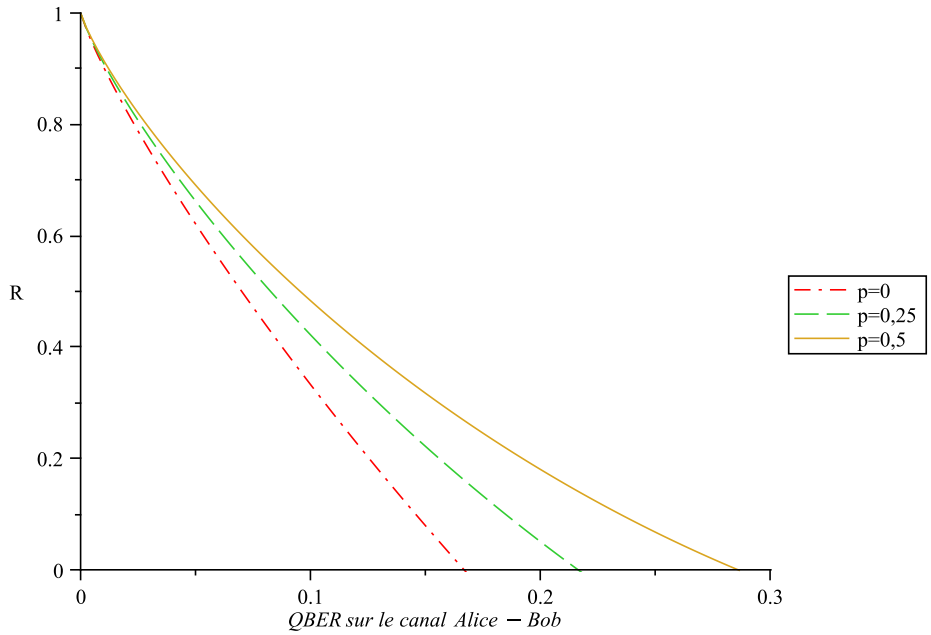


FIGURE 5.5 – Taux de clé secrète R en fonction du QBER sur le canal Alice/Bob pour différentes valeurs de bruit dans la mémoire pour le protocole *six-states*.

quantique augmente.

L'attaque avec mémoire quantique bruitée que nous venons de décrire est meilleure que l'attaque optimale sans mémoire calculée dans le chapitre précédent lorsque le bruit p dans la mémoire est inférieur à $19,6$ %. La contrainte imposée à l'espion par ce modèle d'attaque est moins gênante pour lui sur le protocole *six-states* que pour BB84. Une explication de cette observation est qu'il est plus avantageux d'attendre la révélation des bases avant de mesurer pour le protocole *six-states* où l'incertitude sur le choix de la base est a priori plus grande que pour BB84.

5.2.3 Limites de cette approche

Au vu des résultats obtenus dans les sous-sections précédentes, il apparaît clairement que le modèle d'attaque considéré est très contraignant sur l'espion et ne permet pas de juger de ses capacités réelles. L'obligation d'utiliser sa mémoire quantique quel que soit son niveau de bruit rend l'attaque inefficace dès que le bruit dépasse 4 % et $19,6$ % pour BB84 et *six-states* par rapport à une attaque sans mémoire.

Il est donc nécessaire de permettre à l'espion d'utiliser au mieux sa mémoire quantique bruitée en lui laissant la possibilité d'utiliser une stratégie mixte avec le stockage d'une partie de ses états quantiques dans la mémoire et la mesure immédiate de l'autre partie. C'est ce modèle que nous étudions dans la section suivante.

Malheureusement la description explicite d'une telle attaque est impossible en raison du trop grand nombre de paramètres impliqués. Il convient donc d'utiliser une autre méthode pour prouver la sécurité des protocoles de distribution quantique de clés dans ce modèle plus général de la mémoire bruitée.

5.3 Preuve de sécurité dans le modèle de la mémoire bruitée

Dans cette section, nous allons considérer un modèle très général d'espion dans lequel la seule restriction imposée concerne la mémoire quantique utilisée. En dehors de cela, on suppose que l'espion a accès à une quantité non bornée de puissance de calcul classique et de mémoire classique non bruitée. Cette approche est inspirée des travaux de [Koenig 2009b] sur un modèle similaire appliqué à l'étude de la sécurité de primitives cryptographiques à deux participants telles que la mise en gage quantique ou la transmission inconsciente.

Après avoir présenté quelques résultats utiles à la démonstration, le modèle de sécurité considéré sera détaillé en utilisant le protocole BB84 comme référence. Après avoir obtenu les bornes de sécurité pour ce protocole, les mêmes méthodes seront appliquées dans un deuxième temps aux protocoles *six-states* et SARG04.

5.3.1 Résultats utiles à la démonstration.

Nous présentons ici deux théorèmes qui seront utilisés dans la preuve de sécurité de BB84 dans le modèle de la mémoire bruitée.

Le premier permet de borner l'information contenue par un état quantique après son passage dans un canal bruité. La démonstration de ce théorème se trouve dans [Koenig 2009b].

On considère un état classique-quantique ρ_{XTQ} quelconque (classique sur X et T) et un canal quantique $\mathcal{F} : \mathcal{S}(\mathcal{H}_Q) \longrightarrow \mathcal{S}(\mathcal{H}_{Q_{out}})$. On a alors le résultat suivant :

$$\forall \varepsilon, \varepsilon' \geq 0, \qquad H_{min}^{\varepsilon+\varepsilon'}(X|T\mathcal{F}(Q)) \geq -\log P_{succ}^{\mathcal{F}}\left(\lfloor H_{min}^{\varepsilon}(X|T) - \log\frac{1}{\varepsilon'}\rfloor\right) \tag{5.41}$$

où $P_{\text{succ}}^{\mathcal{F}}(m)$ est la probabilité de succès de la transmission de m bits sur le canal quantique $\mathcal{F}$. Pour un canal quelconque $\mathcal{F} : \mathcal{S}(\mathcal{H}_{\text{in}}) \longrightarrow \mathcal{S}(\mathcal{H}_{Q_{\text{out}}})$ elle est définie formellement de la façon suivante :

$$\forall m \in \mathbb{N}, \qquad P_{\text{succ}}^{\mathcal{F}}(m) = \max_{\{D_x\}_x, \{\rho_x\}_x} \frac{1}{2^m} \sum_{x\in\{0,1\}^m} \text{Tr}\left(D_x \mathcal{F}(\rho_x)\right) \tag{5.42}$$

où la maximisation est faite sur l'ensemble des familles de codes $\{\rho_x\}_{x\in\{0,1\}^m}$ sur l'espace de Hilbert $\mathcal{H}_{\text{in}}$ et l'ensemble des POVMs de décodage $\{D_x\}_{x\in\{0,1\}^m}$ sur $\mathcal{H}_{\text{out}}$.

Cette quantité est la version quantique d'une relation connue en théorie de l'information classique sous le nom de *strong converse theorem*. Ce théorème a été prouvé dans [Wolfowitz 1957] et affirme que la probabilité d'erreur P_e lors d'une transmission à un taux R sur un canal de capacité C tend exponentiellement vers 1 lorsque $R > C$:

$$\exists\ A \in \mathbb{R}_+ \quad \text{tel que} \quad P_e \geq 1 - \frac{4A}{n(R-C)^2} - e^{-n(R-C)}. \tag{5.43}$$

Cela signifie tout simplement que la capacité d'un canal est une limite dure entre un régime où la transmission est parfaitement fiable et un régime où la transmission devient impossible.

Dans le cas quantique, il a été prouvé [Koenig 2009a] qu'un grand nombre de canaux (dont le canal à dépolarisation) vérifient cette propriété. Plus précisément si $\mathcal{N}$ est un canal à dépolarisation alors pour un taux $R = \frac{m}{n}$ supérieur à la capacité classique du canal $C_{\mathcal{N}}$ on a

$$\exists\ \gamma^{\mathcal{N}}(R) > 0 \quad \text{tel que} \quad -\log P_{\text{succ}}^{\mathcal{N}^{\otimes n}}(m) \geq n\gamma^{\mathcal{N}}(R). \tag{5.44}$$

La probabilité de succès décroît ainsi exponentiellement vers 0 lorsque le taux R est supérieur à la capacité classique du canal $C_{\mathcal{N}}$, ce comportement étant identique à la version classique.

Un formule explicite permettant de calculer la quantité $\gamma^{\mathcal{N}}(R)$ est également donnée dans [Koenig 2009a]. Ainsi, pour un canal à dépolarisation $\mathcal{D}_p$ agissant sur des qubits, on peut écrire :

$$\gamma^{\mathcal{D}_p}(R) = \max_{\alpha\geq 1} \frac{\alpha-1}{\alpha}\left(R - 1 + \frac{1}{1-\alpha}\log\left[\left(\frac{p}{2}\right)^{\alpha} + \left(1-\frac{p}{2}\right)^{\alpha}\right]\right). \tag{5.45}$$

Il est intéressant d'étudier le comportement de cette fonction lorsque le bruit dans la mémoire tend vers 0 ou 1. Ainsi, il est assez facile de remarquer que dans le cas d'une mémoire non bruitée

$$\lim_{p\to 0} \gamma^{\mathcal{D}_p}(R) = \max(0, R-1) \tag{5.46}$$

et que au contraire dans le cas d'une mémoire complètement bruitée

$$\lim_{p\to 1} \gamma^{\mathcal{D}_p}(R) = R. \tag{5.47}$$

Le deuxième théorème présenté ici sera également nécessaire pour la démonstration de la preuve de sécurité dans le modèle de la mémoire bruitée. Sa démonstration

peut être trouvée dans [Damgaard 2007].

Soient $Z_1, ..., Z_n$ des variables aléatoires quelconques sur un alphabet $\mathcal{Z}$ et $h \geq 0$ tel que

$$H(Z_i|Z_1 = z_1, ..., Z_{i-1} = z_{i-1}) \geq h \tag{5.48}$$

pour tout $i \in [\![1, n]\!]$ et $z_1, ..., z_{i-1} \in \mathcal{Z}$. Alors pour tout $0 < \lambda < \frac{1}{2}$

$$H_\infty^\varepsilon(Z_1, ..., Z_n) \geq (h - 2\lambda)n, \tag{5.49}$$

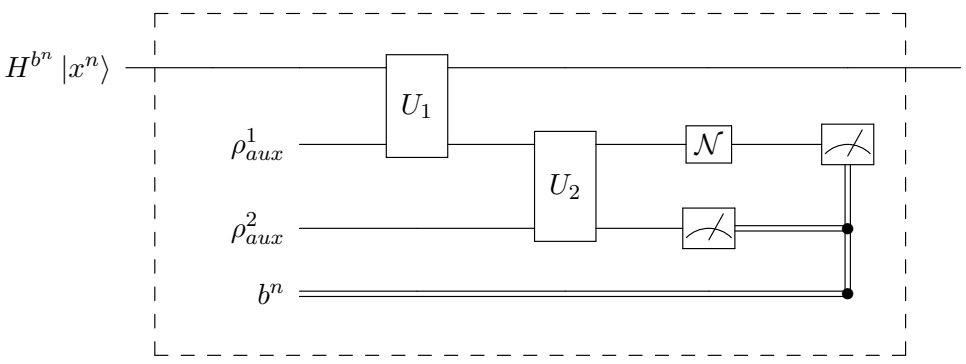
où $\varepsilon = \exp(-\frac{\lambda^2 n}{32 \log(|\mathcal{Z}|/\lambda)^2})$.

5.3.2 Présentation du modèle d'espion avec mémoire quantique bruitée sur le protocole BB84

Pendant la phase de communication quantique de BB84, Alice choisit aléatoirement un bit secret $x \in \{0, 1\}$ à transmettre à Bob. Pour cela elle choisit aléatoirement une base $b \in \{0, 1\}$ et encode le bit secret sur un état quantique $|\phi\rangle_A = H^b |x\rangle$ où H est la transformation de Hadamard. Cet état quantique est ensuite transmis par l'intermédiaire d'un canal quantique à Bob qui le mesure dans une base b' et conserve le résultat pour la phase de réconciliation. Après la mesure de Bob, Alice envoie l'information de la base b et les cas où les bases ne correspondent pas sont éliminés. En ignorant dès le début ces cas non concordants, on peut considérer à partir de maintenant que $b = b'$. Cette opération étant répétée n fois, on note $H^{b^n} |x^n\rangle = H^{b_1} \otimes \cdots \otimes H^{b_n} |x_1 \dots x_n\rangle$ l'état envoyé par Alice.

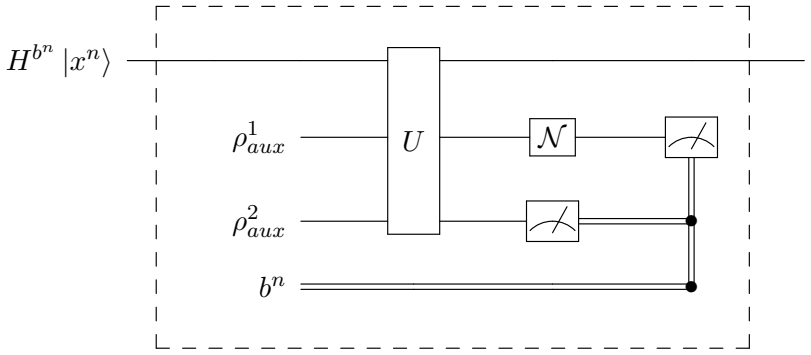
Pendant cette phase de préparation, Eve peut faire interagir l'état envoyé par Alice avec un système auxiliaire ρ^1_{aux} par l'intermédiaire d'une opération unitaire U_1. Elle a alors le choix de mesurer immédiatement et sans bruit l'état auxiliaire $\mathcal{E}(\rho^1_{\text{aux}})$ ou de le stocker dans une mémoire quantique afin de le mesurer ultérieurement. Elle peut également choisir une situation intermédiaire dans laquelle une partie du système est stockée et l'autre partie mesurée. Pour représenter l'ensemble de ces choix, on introduit une deuxième opération unitaire U_2 et un deuxième système auxiliaire ρ^2_{aux}.

Ce modèle d'attaque peut être schématisé par le circuit quantique suivant :



(5.50)

L'utilisation de deux opérations unitaires U_1 et U_2 permet de mieux comprendre le choix offert à Eve de stocker une partie de son système auxiliaire dans sa mémoire quantique et de mesurer l'autre partie. Néanmoins il est possible de simplifier ce circuit sans perte de généralité en ne considérant qu'une seule interaction unitaire U. Dans ce cas le circuit quantique décrivant le modèle de sécurité est le suivant :



(5.51)

Dans ce modèle, le choix de la mesure est optimisé en fonction de l'information classique obtenue lors de la première mesure et de l'information sur la base transmise pendant la phase de réconciliation.

Modélisation de la mémoire quantique.

On reprend ici la modélisation introduite dans la section précédente : ainsi le canal quantique $\mathcal{N}$ peut être décrit par un produit tensoriel de νn canaux $\mathcal{M}$ agissant sur des qubits de telle sorte que

$$\mathcal{N} = \mathcal{M}^{\otimes \nu n}. \tag{5.52}$$

Il sera intéressant d'étudier le cas particulier d'une mémoire quantique modélisée par canal à dépolarisation. Ce canal est paramétré par un bruit $p \in [0, 1]$ et peut s'écrire :

$$\begin{array}{rcl} \mathcal{D}_p : \mathcal{S}(\mathbb{C}^2) & \longrightarrow & \mathcal{S}(\mathbb{C}^2) \\ \rho_{in} & \longmapsto & \rho_{out} = \frac{p\mathbb{I}}{2} + (1-p)\rho_{in}. \end{array} \tag{5.53}$$

Notations.

- On note $X = (X_1, \ldots, X_n)$ la variable aléatoire représentant les n bits secrets choisis par Alice.

- On note E l'ensemble du système de l'espion. Cet ensemble peut être décomposé en 3 parties :

  - $Q_{\text{out}} = \mathcal{N}(Q_{\text{in}})$ qui représente l'état quantique présent dans la mémoire juste avant la mesure finale,
  - K qui représente l'information classique obtenue lors de la première mesure,
  - B qui représente l'information sur la base utilisée et qui est dévoilée pendant la phase de réconciliation.

Calcul d'une borne supérieure sur l'information accessible à l'espion.

Dans le modèle d'attaque décrit par le circuit 5.51, l'état du système juste avant la mesure finale de l'espion est représenté par l'état $\rho_{XE} = \rho_{XKB\mathcal{N}(Q_{\text{in}})}$ avec les notations introduites précédemment.

Nous pouvons alors utiliser un résultat de [Renner 2005a] pour affirmer qu'une clé secrète de longueur l peut être distillée si la condition suivante est vérifiée :

$$l \leq H_{\min}^{\varepsilon}(X|E) - H_{\max}(I_{ec}) - 2\log\frac{1}{\varepsilon}. \tag{5.54}$$

où $\varepsilon > 0$ est le paramètre de sécurité.

On peut tout d'abord calculer une borne supérieure sur $H_{\max}(I_{ec})$ où I_{ec} représente l'information divulguée lors de la phase de correction d'erreur. Sachant que le taux d'erreur sur le canal Alice-Bob est le QBER noté Q, en supposant que le code correcteur d'erreur utilisé ne divulgue pas plus d'information que nécessaire on obtient comme dans [Kraus 2005] que

$$H_{\max}(I_{ec}) \leq n.h(Q) \tag{5.55}$$

où on rappelle que $h(.)$ est la fonction entropie binaire.

L'objectif de la preuve est maintenant d'obtenir une borne inférieure sur $H_{\min}^{\varepsilon}(X|E)$, qui quantifie la méconnaissance de l'espion vis à vis de la clé secrète.

Afin de caractériser la perte d'information causée par le bruit dans la mémoire quantique $\mathcal{N}$ de l'espion, on applique le résultat 5.41 à l'état $\rho_{XE} = \rho_{XKB\mathcal{N}(Q_{\text{in}})}$ où on choisit $\mathcal{F} = \mathcal{N}$ et $T = KB$. On obtient alors

$$H_{\min}^{\varepsilon}(X|E) = H_{\min}^{\frac{\varepsilon}{2}+\frac{\varepsilon}{2}}(X|KB\mathcal{N}(Q_{\text{in}})) \tag{5.56}$$

$$\geq -\log P_{\text{succ}}^{\mathcal{N}}\left(\lfloor H_{\min}^{\frac{\varepsilon}{2}}(X|KB) - \log\frac{2}{\varepsilon}\rfloor\right). \tag{5.57}$$

On peut simplifier cette expression en notant que d'une part $\lfloor x \rfloor > x - 1$ et d'autre part la fonction $-\log P_{\text{succ}}^{\mathcal{N}}$ est croissante. On a peut alors réécrire l'inégalité précédente de la façon suivante :

$$H_{\min}^{\varepsilon}(X|E) \geq -\log P_{\text{succ}}^{\mathcal{N}}\left(H_{\min}^{\frac{\varepsilon}{2}}(X|KB) - \log\frac{4}{\varepsilon}\right). \tag{5.58}$$

Cette expression nous permet d'obtenir une borne inférieure sur $H_{\min}^{\varepsilon}(X|E)$ dans laquelle le canal bruité n'intervient que par l'intermédiaire de la fonction $P_{\text{succ}}^{\mathcal{N}}$ que nous pouvons évaluer à partir de la capacité classique du canal représentant la mémoire. L'évaluation de cette borne inférieure est ainsi considérablement simplifiée par rapport au calcul direct de $H_{\min}^{\varepsilon}(X|E)$.

Il faut maintenant borner inférieurement la quantité $H_{\min}^{\varepsilon}(X|KB)$. Cette min-entropie lissée représente l'incertitude sur la clé secrète X connaissant le résultat de la mesure K et l'information B sur la base utilisée par Alice.

Les premières méthodes utilisées au cours de nos recherches pour borner inférieurement cette quantité se sont révélées infructueuses et ont fourni des bornes qui n'étaient pas assez bonnes pour obtenir des résultats intéressants sur le domaine de sécurité des protocoles de distribution quantique de clés. Nous présentons ici les différentes méthodes qui ont permis d'obtenir ces premiers résultats ainsi que les raisons de leur faiblesse.

Première approximation de $H_{\min}^{\varepsilon}(X|KB)$ par la relation d'incertitude sous forme entropique.

Une première borne inférieure sur $H_{\min}^{\varepsilon}(X|KB)$ peut se calculer en utilisant un résultat de [Koenig 2009b]. En effet, d'après le résultat (19) de cet article, pour tout POVM utilisé par Eve lors de sa première mesure, dont le résultat est représenté par K, l'inégalité suivante est vérifiée :

$$\forall \delta \in]0, \frac{1}{2}[\qquad H_{\min}^{\varepsilon}(X|KB) \geq n(\frac{1}{2} - 2\delta) \tag{5.59}$$

où le paramètre de lissage ε est donné par la relation

$$\varepsilon = \exp\left(-\frac{\delta^2 n}{32(2+\log\frac{1}{\delta})^2}\right). \tag{5.60}$$

Cela signifie que le paramètre δ peut être choisi arbitrairement proche de 0 avec un paramètre de lissage suffisamment petit lorsque la taille de la clé n tend vers l'infini. Par exemple, en choisissant la valeur $\varepsilon = 10^{-9}$ on peut choisir $\delta = 10^{-2}$ lorsque $n \geq n_{\min} = 5.10^8$, ce qui est une taille de clé accessible.

On considère maintenant que le canal quantique utilisé est de la forme $\mathcal{N} = \mathcal{D}_p^{\otimes \nu n}$. En reprenant l'équation 5.58 et en y injectant 5.59, on obtient alors :

$$H_{\min}^{\varepsilon}(X|E) \geq -\log P_{\text{succ}}^{\mathcal{D}_p^{\otimes \nu n}}\left(n(\frac{1}{2}-2\delta) - \log\frac{4}{\varepsilon}\right). \tag{5.61}$$

où la relation 5.60 est toujours vérifiée.

On définit alors le taux $R = \frac{1}{2} - 2\delta$. En appliquant le résultat 5.44 on peut écrire

$$H_{\min}^{\varepsilon}(X|E) \geq n\nu.\gamma^{\mathcal{D}_p}(\frac{R}{\nu}). \tag{5.62}$$

En reprenant la condition 5.54 on peut alors calculer la longueur limite $l_{\lim}$ de la clé au delà de laquelle la sécurité n'est plus assurée :

$$l_{\lim} = H_{\min}^{\varepsilon}(X|E) - H_{\max}(I_{ec}) = n(\nu.\gamma^{\mathcal{D}_p}(\frac{R}{\nu}) - h(Q)). \tag{5.63}$$

Cette longueur limite dépend du QBER observé par Alice et Bob sur leur canal noté Q, du bruit de la mémoire quantique p et du taux de stockage ν. Dans le cas limite d'une mémoire non bruitée, si $\nu \geq R \approx \frac{1}{2}$ alors le taux de clé est nul. Si au contraire $\nu < R$ alors on peut écrire :

$$\lim_{p\to 0} \frac{l_{\lim}}{n} \leq R - \nu - h(Q). \tag{5.64}$$

Dans le cas le plus favorable pour Alice et Bob où $\nu = 0$ c'est à dire lorsque l'espion n'utilise pas sa mémoire pourtant sans bruit, le taux de clé secrète

$$t_{\text{sec}} = \frac{l_{\lim}}{n} \approx \frac{1}{2} - h(Q) \tag{5.65}$$

est deux fois plus petit que le taux de clé secrète obtenu par [Shor 2000] dans le cas des attaques les plus générales.

Ce résultat provient du fait que la borne choisie pour $H_{\min}^{\varepsilon}(X|KB)$ (relation 5.59) n'est pas assez bonne. La raison principale est que cette borne ne fait pas

intervenir le QBER sur le canal quantique. Même pour un QBER nul cette méthode ne limite pas la connaissance de l'espion à zéro comme c'est pourtant forcément le cas : en effet, l'espion perturbe forcément l'état quantique envoyé par Alice en obtenant de l'information sur cet état.

Au final, le résultat obtenu ne permet pas d'améliorer les bornes de sécurité déjà connues. Il convient donc d'affiner l'estimation de cette min-entropie en particulier en faisant intervenir le QBER maximum que peut produire l'attaque d'Eve sur le canal quantique.

Utilisation de la borne provenant de la relation d'incertitude généralisée aux entropies lissées.

Une façon d'améliorer la borne inférieure sur $H^{\varepsilon}_{\min}(X|KB)$ provient de l'utilisation d'un résultat obtenu récemment [Tomamichel 2011] sur la relation d'incertitude généralisée aux entropies lissées. Le principal résultat de cet article peut s'écrire de la façon suivante :

On considère un état quantique tripartite ρ_{ABC} et deux POVMs $\mathbb{X}$ et $\mathbb{Z}$ agissant sur A avec pour éléments $\{M_x\}_{x\in\mathcal{X}}$ et $\{N_z\}_{z\in\mathcal{Z}}$. Alors on peut dire que

$$\forall \varepsilon \geq 0, \qquad H^{\varepsilon}_{min}(X|B) + H^{\varepsilon}_{max}(Z|C) \geq \log \frac{1}{c} \tag{5.66}$$

où c est le recouvrement entre les POVMs défini par $c = \max_{x,z} \left\| \sqrt{M_x}\sqrt{N_z} \right\|^2_{\infty}$.

On applique alors ce théorème à l'état $\rho_{XEY} = \rho_{XKBY}$ où Y représente la chaîne de bits obtenue par Bob pendant la phase de communication quantique. Les POVMs $\mathbb{X}$ et $\mathbb{Z}$ représentent quant à eux les 2 bases utilisées par Alice lors de sa mesure. Dans le cas de BB84 on peut alors facilement calculer la valeur du recouvrement : $c = \frac{1}{2}$. On obtient alors l'inégalité suivante :

$$H^{\varepsilon}_{\min}(X|E) \geq n - H^{\varepsilon}_{\max}(Z|Y) = n - H^{\varepsilon}_{\max}(X|Y), \tag{5.67}$$

la dernière égalité provenant du fait que le choix de la base de mesure par Alice n'a pas d'influence sur la corrélation entre les résultats d'Alice et de Bob. Sachant que $H^{\varepsilon}_{\max}(X|Y) \leq n.h(Q)$ on obtient finalement

$$H^{\varepsilon}_{\min}(X|E) \geq n(1 - h(Q)). \tag{5.68}$$

En utilisant la même méthode que celle qui a conduit au calcul de l'équation 5.64 on trouve le taux de clé secrète

$$t_{\text{sec}} \approx 1 - 2h(Q). \tag{5.69}$$

Ce taux n'est pas meilleur que celui obtenu dans le cas général où l'espion n'est pas limité. On en déduit que la borne utilisée pour $H_{\min}^{\varepsilon}(X|KB)$ n'est pas encore assez bonne pour fournir une preuve de sécurité meilleure que celles existantes.

Utilisation de la borne provenant de l'attaque optimale sans mémoire.

Les bornes inférieures sur $H_{\min}^{\varepsilon}(X|KB)$ utilisées dans les pages précédentes surestimaient l'information accessible à l'espion en ne prenant pas suffisamment en compte le fait que l'ensemble des interactions utilisables par Eve est limité par le QBER pouvant être généré sur le canal Alice-Bob. Cette quantité d'information décroît rapidement avec Q lorsque Eve n'a pas de mémoire quantique comme cela a été prouvé dans le chapitre 4 sur les attaques optimales sans mémoire. Or la quantité $H_{\min}^{\varepsilon}(X|KB)$ correspond justement à la quantité d'information accessible à Eve lors de la première mesure, sans utilisation de la mémoire quantique. L'idée est donc d'utiliser les résultats obtenus dans le chapitre 4 pour borner $H_{\min}^{\varepsilon}(X|KB)$.

Pour cela on commence par appliquer la règle de chaînage 1.168 à $H_{\min}^{\varepsilon}(X|KB)$. On obtient alors l'inégalité

$$H_{\min}^{\varepsilon}(X|KB) \geq H_{\min}^{\varepsilon}(XKB) - H_{\max}(KB). \tag{5.70}$$

Pour simplifier les notations, on pose $Z = XKB$. L'objectif est maintenant dans un premier temps de borner la min-entropie lissée $H_{\min}^{\varepsilon}(Z)$.

On souhaite pour cela appliquer le théorème 5.49. On considère alors la quantité $H(Z_i|Z_1 = z_1, ..., Z_{i-1} = z_{i-1})$ où $Z = (Z_1, ..., Z_n)$.

En utilisant 1.32 on peut développer cette expression de la façon suivante :

$$H(Z_i|Z_1 = z_1, ..., Z_{i-1} = z_{i-1}) = H(K_i|X_iB_i) + H(X_i|B_i) + H(B_i) \tag{5.71}$$

Les deux derniers termes de cette expression se calculent facilement. En effet, les variables aléatoires X_i et B_i étant indépendantes et uniformément distribuées, on a

$$H(X_i|B_i) = H(X_i) = \log|\mathcal{X}| \tag{5.72}$$
$$H(B_i) = \log|\mathcal{B}| \tag{5.73}$$

Dans le cas de BB84 où $|\mathcal{B}| = |\mathcal{X}| = 2$ on a alors $H(X_i|B_i) + H(B_i) = 2$.

Pour calculer le premier terme de cette expression, on introduit les probabilités conditionnelles $p(K_i = k_i|X_i = x_i, B_i = b_i) = p_{k_i,x_ib_i}$ qui représentent la probabilité pour Eve de mesurer k_i lorsque l'état envoyé par Alice est $H^{b_i}|x_i\rangle$. Ces probabilités

se déduisent directement du POVM utilisé par Eve lors de sa première mesure. Ainsi, si on note $\{M_k\}_{k\in\mathcal{K}}$ le POVM utilisé par Eve et $\rho^E_{x_i b_i}$ l'état mesuré par Eve, les probabilités $p_{k_i,x_i b_i}$ s'écrivent

$$p_{k_i,x_i b_i} = \mathrm{Tr}\left(M_{k_i}\rho^E_{x_i b_i}\right). \tag{5.74}$$

En optimisant de la même manière que dans le chapitre 4 l'attaque d'Eve sur l'ensemble des POVMs et sur l'ensemble des états $\rho^E_{x_i b_i}$ possibles pour un QBER donné Q alors on obtient l'inégalité

$$H(K_i|X_i B_i) \geq \min_{\{M_k\},\rho^E_{x_i b_i}} \left[-\frac{1}{4}\sum_{k_i,x_i,b_i} p_{k_i,x_i b_i}\log p_{k_i,x_i b_i}\right] = \kappa(Q). \tag{5.75}$$

où on a noté $\kappa(Q)$ le résultat de l'optimisation que nous avons déjà définie au chapitre 4 page 81. Finalement en rassemblant 5.72, 5.73 et 5.75 on obtient l'inégalité

$$H(Z_i|Z_1 = z_1, ..., Z_{i-1} = z_{i-1}) \geq 2 + \kappa(Q) \tag{5.76}$$

qui nous permet d'appliquer le théorème 5.49 et d'obtenir que

$$H^\varepsilon_{\min}(XKB) \geq (2 + \kappa(Q) - 2\lambda)n \tag{5.77}$$

où $\varepsilon = \exp(-\frac{\lambda^2 n}{32\log(16/\lambda)^2})$.

Pour finir, on peut borner le terme de droite de l'expression 5.70 par la relation

$$H_{\max}(KB) \leq (\log|\mathcal{K}| + \log|\mathcal{B}|). \tag{5.78}$$

On peut alors injecter les résultats 5.77 et 5.78 dans 5.70 afin d'obtenir la borne

$$H^\varepsilon_{\min}(X|KB) \geq (\kappa(Q) - 1 - 2\lambda)n. \tag{5.79}$$

On peut alors intégrer ce résultat dans l'équation 5.58 pour obtenir

$$H^\varepsilon_{\min}(X|E) \geq -\log P^{\mathcal{D}_p^{\otimes\nu n}}_{\mathrm{succ}}\left(\left[\kappa(Q) - 1 - 2\lambda\right]n - \log\frac{4}{\varepsilon}\right) \tag{5.80}$$

Pour calculer la fonction $P^{\mathcal{D}_p^{\otimes\nu n}}_{\mathrm{succ}}$ on utilise le résultat 5.44. Ainsi, en posant $R = \kappa(Q) - 1 - 2\lambda$ on peut écrire

$$H^\varepsilon_{\min}(X|E) \geq -\log P^{\mathcal{D}_p^{\otimes\nu n}}_{\mathrm{succ}}(nR) \geq \nu n\gamma^{\mathcal{D}_p}(\frac{R}{\nu}), \tag{5.81}$$

où on rappelle que ν représente le taux de stockage de la mémoire quantique de l'espion, p est le paramètre définissant la quantité de bruit dans la mémoire quantique et la fonction $\gamma^{\mathcal{D}_p}(\cdot)$ est définie par la relation :

$$\gamma^{\mathcal{D}_p}(x) = \max_{\alpha \geq 1} \frac{\alpha - 1}{\alpha} \left(x - 1 + \frac{1}{1-\alpha} \log \left[\left(\frac{p}{2}\right)^{\alpha} + \left(1 - \frac{p}{2}\right)^{\alpha} \right] \right). \tag{5.82}$$

Finalement le taux de clé secrète t_{sec} est donné par

$$t_{\text{sec}} = \max(0, \nu\gamma^{\mathcal{D}_p}(\frac{R}{\nu}) - h(Q)). \tag{5.83}$$

A partir de cette relation, il est possible d'étudier les cas limites de mémoire parfaite ou au contraire complètement bruitée respectivement représentés par $p \to 0$ et $p \to 1$. Sachant que :

$$\lim_{p \to 0} \gamma^{\mathcal{D}_p}(x) = \max(0, x - 1) \tag{5.84}$$

et

$$\lim_{p \to 1} \gamma^{\mathcal{D}_p}(x) = x \tag{5.85}$$

on peut en déduire que dans la limite d'une mémoire quantique parfaite ($p = 0$) le taux de clé secrète se réduit à

$$t_{\text{sec}} = \max(0, R - \nu - h(Q)). \tag{5.86}$$

En particulier pour un taux de stockage $\nu = 1$ on a $t_{\text{sec}} = 0$ quelle que soit la valeur du QBER. Cela signifie que pour une mémoire parfaite et un taux de stockage de 1 notre preuve de sécurité ne permet pas de garantir la sécurité du protocole.

Dans le cas limite d'une mémoire complètement bruitée ($p = 1$) le taux de clé se réduit à

$$t_{\text{sec}} = \kappa(Q) - 1 - h(Q), \tag{5.87}$$

ce qui correspond exactement au cas déjà étudié dans le chapitre 4 des attaques optimales sans mémoire.

Pour analyser ce résultat, on peut par exemple étudier l'évolution du QBER critique au delà duquel le taux de clé secrète devient nul. Ainsi on a tracé sur la figure 5.6 le QBER critique pour BB84 pour trois valeurs de ν en fonction du bruit p dans la mémoire de l'adversaire. La ligne à 11 % représente le QBER critique obtenu par la preuve inconditionnelle de sécurité de BB84 contre un adversaire non limité. La ligne à 15,4 % représente le QBER critique obtenu dans le modèle de l'attaquant sans mémoire.

On remarque tout d'abord que pour un taux de stockage $\nu = 1$ le modèle de la mémoire bruitée permet d'étendre le domaine de sécurité par rapport à la preuve de

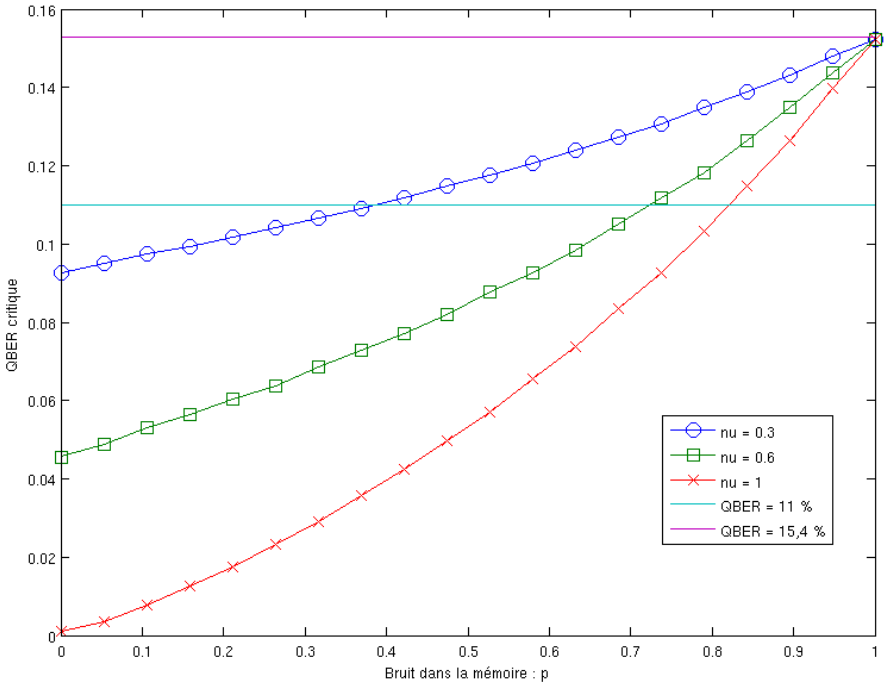


FIGURE 5.6 – QBER critique pour BB84 pour trois valeurs de ν en fonction du bruit p dans la mémoire de l'adversaire.

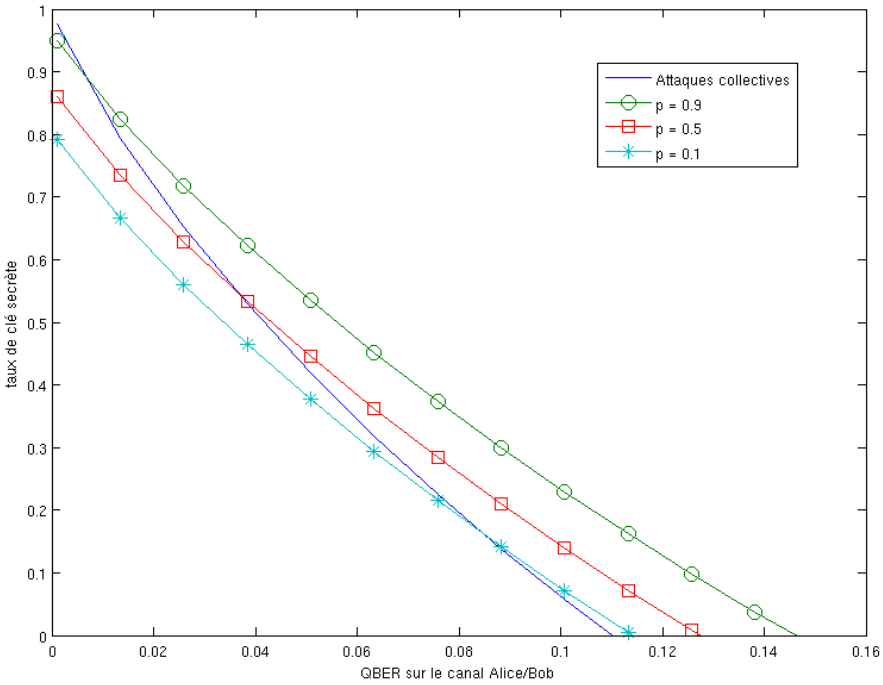


FIGURE 5.7 – Taux de clé secrète pour BB84 pour trois valeurs de bruit p dans la mémoire et un taux de stockage $\nu = 0.2$ en fonction du QBER sur le canal Alice/Bob.

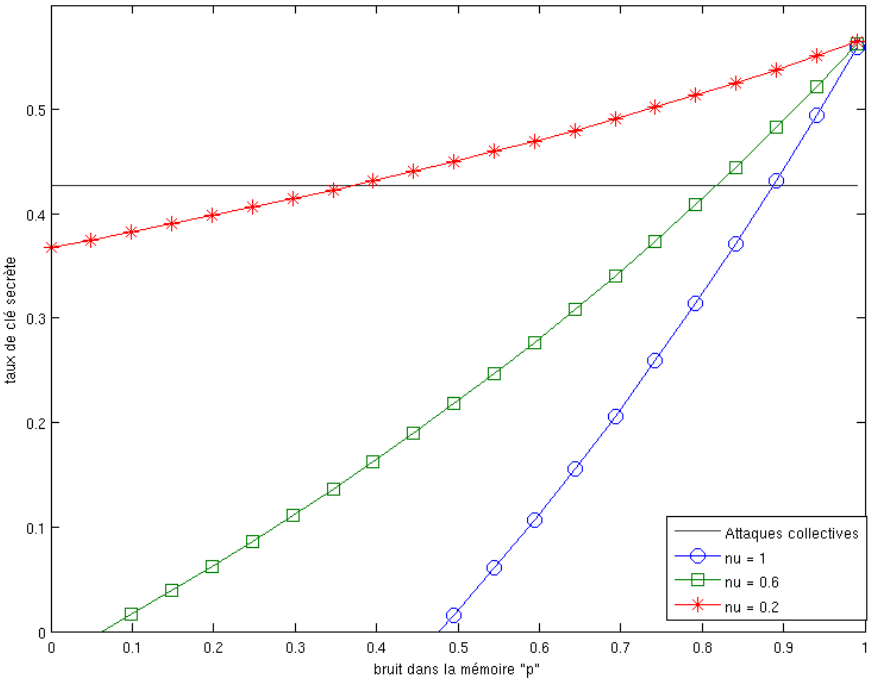


FIGURE 5.8 – Taux de clé secrète pour BB84 pour trois valeurs de taux de stockage nu et un QBER fixé à 5 % en fonction du bruit p dans la mémoire.

sécurité inconditionnelle à partir d'un bruit dans la mémoire supérieur à $0,82$. Idéalement, le cas de la mémoire parfaite devrait aboutir au même résultat que la preuve inconditionnelle de sécurité de BB84 qui conduit à un QBER critique de 11 %. Or la preuve de sécurité présentée ici ne permet pas d'atteindre ces performances. L'information accessible à l'espion est donc surestimée. Malgré cette surestimation, le modèle permet tout de même d'étendre en partie le domaine de sécurité lorsque le bruit dans la mémoire quantique est supérieur à $0,82$ pour un taux de stockage égal à 1.

En revanche, pour un taux de stockage $\nu \leq 0,20$ le modèle de la mémoire bruitée permet d'étendre le domaine de sécurité au delà de 11 % quelle que soit la valeur du bruit dans la mémoire quantique.

On peut s'intéresser plus particulièrement à cette valeur du taux de stockage : on a ainsi tracé sur la figure 5.7 le taux de clé secrète pour plusieurs valeurs de bruit en fonction du QBER. Dans ces conditions, le taux de clé secrète dans le modèle de la mémoire bruitée est quasiment toujours supérieur au taux de clé t_{coll} calculé dans la preuve inconditionnelle. Plus précisément, pour $\nu = 0,2$ et $p = 0,9$, le taux de clé secrète t_{sec} est supérieur à t_{coll} dès lors que le QBER sur le canal Alice/Bob est supérieur à 1 %.

Enfin, une dernière façon d'analyser ces résultats est de calculer le taux de clé secrète pour un QBER fixé à une valeur habituelle rencontrée dans les expériences sur le terrain. On choisit ici la valeur de 5 %. Dans ce cas on peut calculer $t_{\text{coll}} = 1 - 2h(0.05) = 0.43$. On a tracé dans la figure 5.8 le taux de clé secrète pour un QBER de 5 % pour trois valeurs de taux de stockage en fonction du bruit p.

On voit sur ce graphe que pour un taux de stockage $\nu = 0,2$ le taux de clé secrète dans le modèle de la mémoire bruitée est supérieur à $t_{\text{coll}} = 0.43$ dès lors que le bruit dans la mémoire p est supérieur à $0,37$.

Influence comparée des paramètres ν et p caractérisant la mémoire quantique.

Il est intéressant de remarquer que les paramètres caractérisant le taux de stockage et le bruit de la mémoire quantique peuvent être modifiés d'une façon telle que le taux de clé secrète final est inchangé. Par exemple en observant le graphe 5.6 on peut remarquer que les couples de paramètres $(\nu = 0,3, p = 0,39)$, $(\nu = 0,6, p = 0,72)$ et $(\nu = 1, p = 0,82)$ aboutissent au même taux de clé et donc au même QBER critique au delà duquel il n'est plus possible de distiller une clé secrète. Grossièrement on peut dire qu'une petite quantité de mémoire quantique peu bruitée est équivalente à une plus grande quantité de mémoire plus bruitée.

Ce phénomène est assez simple à comprendre : on peut tout à fait imaginer

qu'un adversaire en possession d'une certaine quantité de mémoire quantique bruitée puisse améliorer la qualité de sa mémoire en employant des codes correcteurs d'erreur quantiques au prix d'une diminution de la quantité de mémoire disponible en raison de la redondance de ces codes.

5.3.3 Présentation du modèle d'attaque sur le protocole "six-states"

Le protocole de distribution quantique de clés *six-states* est une version modifiée [Lo 2001, Bechmann-Pasquinucci 1999] de BB84 auquel une base supplémentaire a été ajoutée. Dans ce protocole, Alice peut choisir parmi les 3 bases mutuellement non biaisées (MUB an anglais pour *Mutually Unbiased Bases*) suivantes : $\{|0\rangle, |1\rangle\}$, $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ et $\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\}$.

On note habituellement ces 3 bases respectivement $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ et $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$. Ce choix d'une troisième base permet de simplifier l'étude de la sécurité de ce protocole en rendant le problème symétrique. De plus, au prix d'un taux de réjection plus important que pour BB84 (2/3 au lieu de 1/2) pendant la phase de tamisage (ou phase de *sifting*), la sécurité inconditionnelle de ce protocole a été prouvée jusqu'à un QBER plus élevé que pour BB84 : 12,6 % au lieu de 11 %.

L'étude de la sécurité de ce protocole dans le modèle de la mémoire bruitée reprend en grande partie les résultats présentés dans la section précédente sur BB84. Nous pouvons ainsi utiliser un résultat de [Renner 2005a] pour affirmer qu'une clé secrète de longueur l peut être distillée si la condition suivante est vérifiée :

$$\forall \varepsilon > 0 \qquad l \leq H_{\min}^{\varepsilon}(X|E) - H_{\max}(I_{ec}) - 2\log\frac{1}{\varepsilon}. \tag{5.88}$$

La borne supérieure sur $H_{\max}(I_{ec})$ est identique à celle obtenue pour BB84. Ainsi, pour un QBER sur le canal Alice/Bob égal à Q on peut écrire :

$$H_{\max}(I_{ec}) \leq n.h(Q) \tag{5.89}$$

L'incertitude de l'espion sur la clé $H_{\min}^{\varepsilon}(X|E)$ est par contre différente pour le protocole *six-states*. Néanmoins les premières étapes sont identiques à celles déjà présentées pour BB84. En particulier, les mêmes arguments qui ont permis d'obtenir l'équation 5.58 s'appliquent au protocole *six-states* et on peut écrire :

$$H_{\min}^{\varepsilon}(X|E) \geq -\log P_{\text{succ}}^{\mathcal{N}}\left(H_{\min}^{\frac{\varepsilon}{2}}(X|KB) - \log\frac{4}{\varepsilon}\right). \tag{5.90}$$

Il faut maintenant borner inférieurement la quantité $H_{\min}^{\varepsilon}(X|KB)$. On rappelle que cette min-entropie lissée représente l'incertitude d'Eve sur la clé secrète X sachant qu'elle a accès au résultat de sa mesure K et à l'information B sur la base utilisée par Alice.

Tout comme pour BB84, en appliquant la règle de chaînage 1.168 à $H_{\min}^{\varepsilon}(X|KB)$ on obtient l'inégalité

$$H_{\min}^{\varepsilon}(X|KB) \geq H_{\min}^{\varepsilon}(Z) - H_{\max}(KB). \tag{5.91}$$

où on a posé $Z = XKB$. L'objectif est maintenant dans un premier temps de borner la min-entropie lissée $H_{\min}^{\varepsilon}(Z)$.

Comme précédemment on considère alors la quantité $H(Z_i|Z_1 = z_1, ..., Z_{i-1} = z_{i-1})$ où $Z = (Z_1, ..., Z_n)$ qu'il est possible de développer sous la forme

$$H(Z_i|Z_1 = z_1, ..., Z_{i-1} = z_{i-1}) = H(K_i|X_iB_i) + H(X_i|B_i) + H(B_i). \tag{5.92}$$

Les variables aléatoires X_i et B_i étant indépendantes et uniformément distribuées, on a

$$\begin{aligned} H(X_i|B_i) &= H(X_i) = \log|\mathcal{X}| && (5.93)\\ H(B_i) &= \log|\mathcal{B}| && (5.94) \end{aligned}$$

Dans le cas du protocole *six-states* où $|\mathcal{B}| = 3$ et $|\mathcal{X}| = 2$ on a alors $H(X_i|B_i) + H(B_i) = 1 + \log 3$.

Pour calculer $H(K_i|X_iB_i)$, on introduit les probabilités conditionnelles $p(K_i = k_i|X_i = x_i, B_i = b_i) = p_{k_i,x_ib_i}$ qui représentent la probabilité pour Eve de mesurer k_i lorsque l'état envoyé par Alice est $H^{b_i}|x_i\rangle$. Ces probabilités se déduisent directement du POVM utilisé par Eve lors de sa première mesure. Ainsi, si on note $\{M_k\}_{k\in\mathcal{K}}$ le POVM utilisé par Eve et $\rho_{x_ib_i}^E$ l'état mesuré par Eve, les probabilités p_{k_i,x_ib_i} s'écrivent

$$p_{k_i,x_ib_i} = \mathrm{Tr}\left(M_{k_i}\rho_{x_ib_i}^E\right). \tag{5.95}$$

Comme cela a été calculé dans le chapitre 4, l'état $\rho_{x_ib_i}^E$ représentant le système de l'espion n'est pas le même pour le protocole *six-states* que pour BB84. En effet, l'utilisation d'une troisième base et donc d'une troisième équation reliant le QBER aux paramètres de l'attaque d'Eve fait que le seul degré de liberté restant concernant l'interaction avec le système auxiliaire est le QBER sur le canal Alice/Bob.

En optimisant de la même manière que dans le chapitre 4 l'attaque d'Eve sur l'ensemble des POVMs pour un QBER donné Q et pour le protocole *six-states* alors on obtient l'inégalité

$$H(K_i|X_iB_i) \geq \min_{\{M_k\},\rho_{x_ib_i}^E} \left[-\frac{1}{4}\sum_{k_i,x_i,b_i} p_{k_i,x_ib_i}\log p_{k_i,x_ib_i}\right] = \kappa'(Q). \tag{5.96}$$

où on a noté $\kappa'(Q)$ le résultat de l'optimisation que nous avons déjà défini au chapitre 4 page 86 pour le protocole *six-states*. Finalement en rassemblant 5.93, 5.94 et 5.96 on obtient l'inégalité

$$H(Z_i|Z_1 = z_1, ..., Z_{i-1} = z_{i-1}) \geq 1 + \log 3 + \kappa'(Q) \tag{5.97}$$

qui nous permet d'appliquer le théorème 5.49 et d'obtenir

$$H_{\min}^{\varepsilon}(XKB) \geq (1 + \log 3 + \kappa'(Q) - 2\lambda)n \tag{5.98}$$

où $\varepsilon = \exp(-\frac{\lambda^2 n}{32\log(16/\lambda)^2})$.

On obtient alors finalement la borne

$$H_{\min}^{\varepsilon}(X|KB) \geq (\kappa'(Q) - 1 - 2\lambda)n. \tag{5.99}$$

On peut alors intégrer ce résultat dans l'équation 5.90 pour obtenir

$$H_{\min}^{\varepsilon}(X|E) \geq -\log P_{\text{succ}}^{\mathcal{D}_p^{\otimes \nu n}}\left(\left[\kappa'(Q) - 1 - 2\lambda\right] n - \log\frac{4}{\varepsilon}\right) \tag{5.100}$$

Pour calculer la fonction $P_{\text{succ}}^{\mathcal{D}_p^{\otimes \nu n}}$ on utilise le résultat 5.44. Ainsi, en posant $R = \kappa'(Q) - 1 - 2\lambda$ on peut écrire

$$-\log P_{\text{succ}}^{\mathcal{D}_p^{\otimes \nu n}}(nR) \geq \nu n \gamma^{\mathcal{D}_p}(\frac{R}{\nu}). \tag{5.101}$$

Finalement le taux de clé secrète t_{sec} est donné par

$$t_{\text{sec}} = \nu\gamma^{\mathcal{D}_p}(\frac{R}{\nu}) - h(Q). \tag{5.102}$$

On retrouve pour le protocole *six-states* les mêmes cas limites de mémoire parfaite et mémoire complètement bruitée que pour BB84. Ainsi, dans la limite d'une mémoire quantique parfaite ($p = 0$) le taux de clé secrète se réduit à

$$t_{\text{sec}} = \max(0, \kappa'(Q) - 1 - \nu - h(Q)). \tag{5.103}$$

En particulier pour un taux de stockage $\nu = 1$ on a $t_{\text{sec}} = 0$ quelle que soit la valeur du QBER sur le canal quantique. Comme pour le protocole BB84, pour une mémoire parfaite et un taux de stockage de 1 la preuve de sécurité dans le modèle de la mémoire bruitée ne permet pas de garantir la sécurité du protocole *six-states*.

Dans le cas limite d'une mémoire complètement bruitée ($p = 1$) le taux de clé se réduit à

$$t_{\text{sec}} = \kappa'(Q) - 1 - h(Q), \tag{5.104}$$

ce qui correspond exactement au cas déjà étudié dans le chapitre 4 des attaques optimales sans mémoire sur le protocole *six-states*.

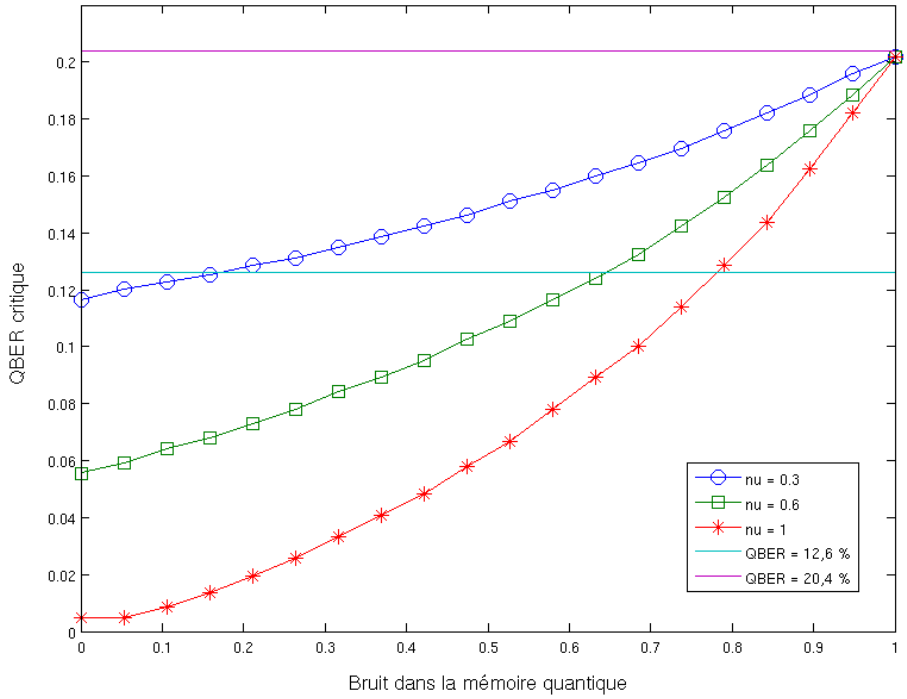


FIGURE 5.9 – QBER critique pour le protocole *six-states* pour trois valeurs de ν en fonction du bruit p dans la mémoire de l'adversaire.

Pour analyser ce résultat, on peut par exemple étudier l'évolution du QBER critique au delà duquel le taux de clé secrète devient nul. Ainsi on a tracé sur la figure 5.9 le QBER critique pour le protocole *six-states* pour trois valeurs de ν en fonction du bruit p dans la mémoire de l'adversaire. La ligne à $12,6$ % représente le QBER critique obtenu par la preuve inconditionnelle de sécurité du protocole *six-states* contre un adversaire non limité [Bruß 1998]. La ligne à $20,4$ % représente le QBER critique obtenu dans le modèle de l'attaquant sans mémoire.

On remarque tout d'abord que pour un taux de stockage $\nu = 1$ le modèle de la mémoire bruitée permet d'étendre le domaine de sécurité par rapport à la preuve de sécurité inconditionnelle à partir d'un bruit dans la mémoire supérieur à $p = 0,77$.

De même pour un taux de stockage $\nu \leq 0,27$ le modèle de la mémoire bruitée permet d'étendre le domaine de sécurité au delà de $12,6$ % quelle que soit la valeur du bruit dans la mémoire quantique.

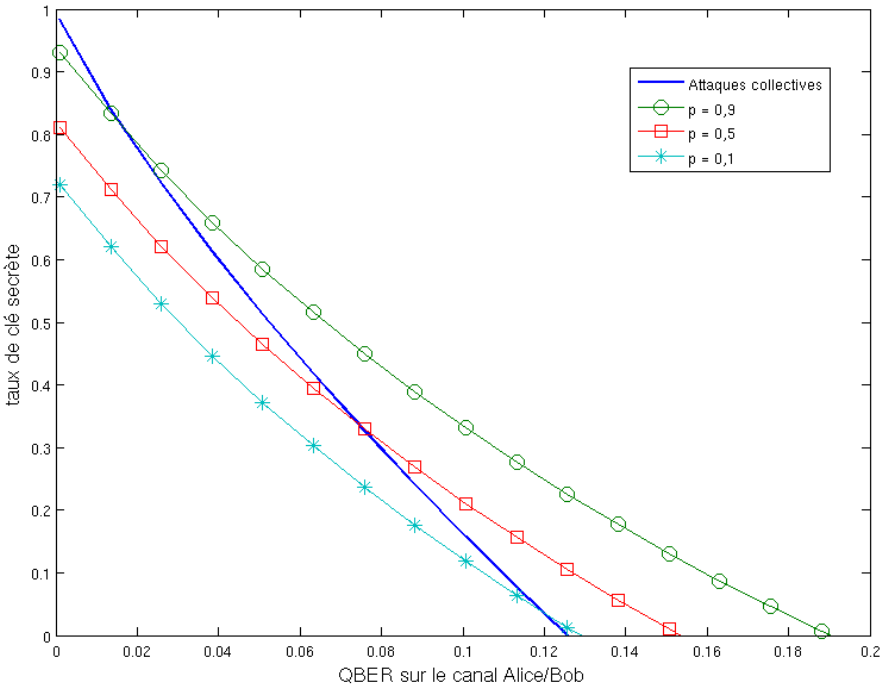


FIGURE 5.10 – Taux de clé secrète pour le protocole *six-states* pour trois valeurs de bruit p dans la mémoire et un taux de stockage $\nu = 0,27$ en fonction du QBER sur le canal Alice/Bob.

On peut s'intéresser plus particulièrement à cette valeur du taux de stockage : on a ainsi tracé sur la figure 5.10 le taux de clé secrète pour plusieurs valeurs de bruit en fonction du QBER pour un taux de stockage fixé $\nu = 0,27$. Dans ces conditions, pour $\nu = 0,27$ et $p = 0,9$, le taux de clé secrète t_{sec} est supérieur à t_{coll} dès lors que le QBER sur le canal Alice/Bob est supérieur à 2 %.

5.3.4 Présentation du modèle d'attaque sur le protocole SARG04

Le protocole de distribution quantique de clés SARG04 [Scarani 2004] utilise les mêmes états quantiques que dans le protocole BB84 mais avec un encodage différent des bits secrets. Rappelons brièvement le fonctionnement de ce protocole. Tout comme dans BB84, Alice prépare un état $H^b |x\rangle$ dans lequel le bit secret est cette fois b au lieu de x comme dans BB84. De cette façon, les états $|0\rangle$ et $|1\rangle$ représentent le bit secret "0" et les états $|+\rangle$ et $|-\rangle$ représentent le bit secret "1".

Par exemple, on considère qu'Alice choisit le bit secret "0" et qu'elle l'encode avec l'état $|0\rangle$ sélectionné aléatoirement parmi l'ensemble $\{|0\rangle, |1\rangle\}$. Le bit sera conservé par Alice et Bob si Bob choisit de mesurer le qubit dans la base $\{|+\rangle, |-\rangle\}$. Dans ce cas Bob peut obtenir un des 2 résultats de mesure de manière équiprobable.

Pendant la phase de réconciliation, Alice va annoncer que l'état quantique envoyé faisait partie de l'ensemble $\{|0\rangle, |+\rangle\}$. Cela permet à Bob d'identifier l'état réellement envoyé comme étant $|0\rangle$ mais ne donne pas d'information à l'espion.

Du point de vue de l'espion, l'attaque est similaire à celle pratiquée sur BB84. La principale différence se trouve dans les paramètres de la purification ρ_{ABE} du protocole intriqué équivalent.

On peut dès lors reprendre directement le résultat 5.80 en remplaçant $\kappa(Q)$ par $\kappa"(Q)$ qui est le résultat de l'optimisation que nous avons déjà défini au chapitre 4 page 89 pour le protocole SARG04 :

$$H_{\min}^{\varepsilon}(X|E) \geq -\log P_{\text{succ}}^{\mathcal{D}_p^{\otimes \nu n}} \left([\kappa"(Q) - 1 - 2\lambda]\, n - \log \frac{4}{\varepsilon} \right) \tag{5.105}$$

Ainsi, en posant $R = \kappa"(Q) - 1 - 2\lambda$ on peut écrire

$$-\log P_{\text{succ}}^{\mathcal{D}_p^{\otimes \nu n}}(nR) \geq \nu n \gamma^{\mathcal{D}_p}(\frac{R}{\nu}). \tag{5.106}$$

Finalement le taux de clé secrète t_{sec} est donné par

$$t_{\text{sec}} = \nu \gamma^{\mathcal{D}_p}(\frac{R}{\nu}) - h(Q). \tag{5.107}$$

Dans la limite d'une mémoire quantique parfaite ($p = 0$), ce taux de clé secrète se réduit à

$$t_{\text{sec}} = \max(0, \kappa"(Q) - 1 - \nu - h(Q)). \tag{5.108}$$

En particulier pour un taux de stockage $\nu = 1$ on a $t_{\text{sec}} = 0$ quelle que soit la valeur du QBER sur le canal quantique. Ainsi, pour une mémoire parfaite et un taux de stockage de 1 la preuve de sécurité dans le modèle de la mémoire bruitée ne permet pas de garantir la sécurité du protocole SARG04.

Dans le cas limite d'une mémoire complètement bruitée ($p = 1$) le taux de clé se réduit à

$$t_{\text{sec}} = \kappa"(Q) - 1 - h(Q), \tag{5.109}$$

ce qui correspond exactement au cas déjà étudié des attaques optimales sans mémoire sur le protocole SARG04.

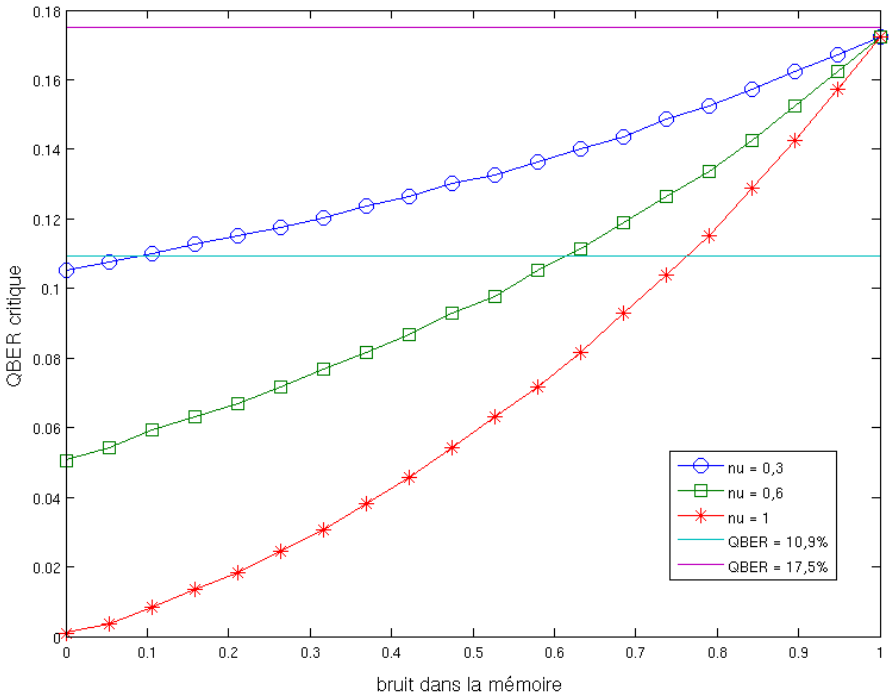


FIGURE 5.11 – QBER critique pour SARG04 pour trois valeurs de ν en fonction du bruit p dans la mémoire de l'adversaire.

Pour analyser ce résultat, on peut par exemple étudier l'évolution du QBER critique au delà duquel le taux de clé secrète devient nul. Ainsi on a tracé sur la

figure 5.11 le QBER critique pour SARG04 pour trois valeurs de ν en fonction du bruit p dans la mémoire de l'adversaire. La ligne à $10,9$ % représente le QBER critique obtenu par la preuve de sécurité inconditionnelle [Branciard 2005] de SARG04 contre un adversaire non limité. La ligne à $17,5$ % représente le QBER critique obtenu dans le modèle de l'attaquant sans mémoire.

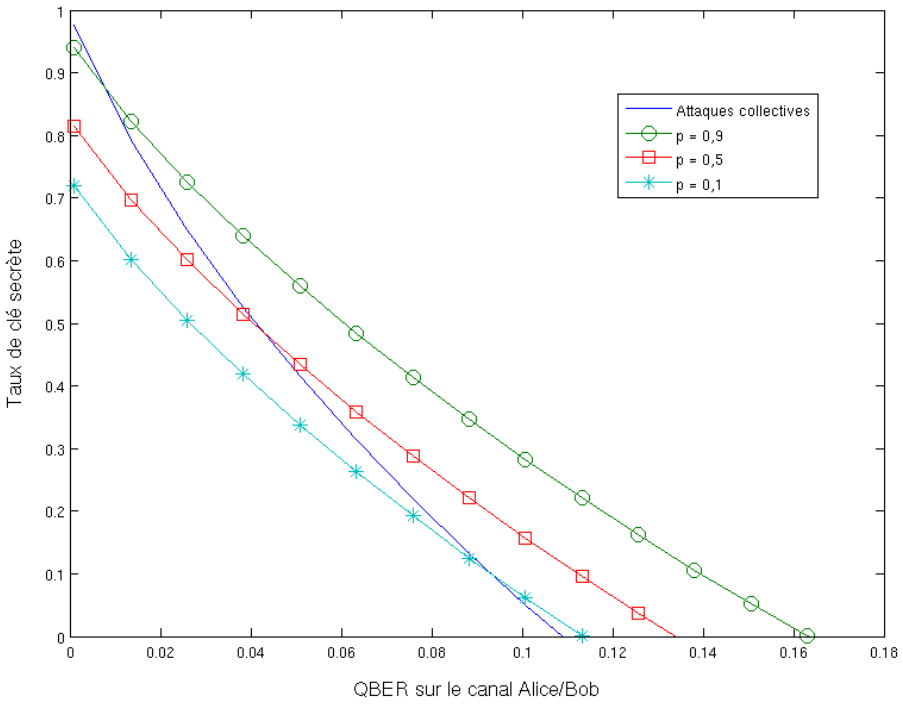


FIGURE 5.12 – Taux de clé secrète pour SARG04 pour trois valeurs de bruit p dans la mémoire et un taux de stockage $\nu = 0,28$ en fonction du QBER sur le canal Alice/Bob.

On remarque tout d'abord que pour un taux de stockage $\nu = 1$ le modèle de la mémoire bruitée permet d'étendre le domaine de sécurité par rapport à la preuve de sécurité inconditionnelle à partir d'un bruit dans la mémoire supérieur à $0,76$.

De même pour un taux de stockage $\nu \leq 0.28$ le modèle de la mémoire bruitée permet d'étendre le domaine de sécurité au delà de $10,9$ % quelle que soit la valeur du bruit dans la mémoire quantique.

On peut s'intéresser plus particulièrement à cette valeur du taux de stockage : on a ainsi tracé sur la figure 5.12 le taux de clé secrète pour plusieurs valeurs de bruit en fonction du QBER. Dans ces conditions, pour $\nu = 0,28$ et $p = 0,9$, le taux de clé secrète t_{sec} est supérieur à t_{coll} dès lors que le QBER sur le canal Alice/Bob

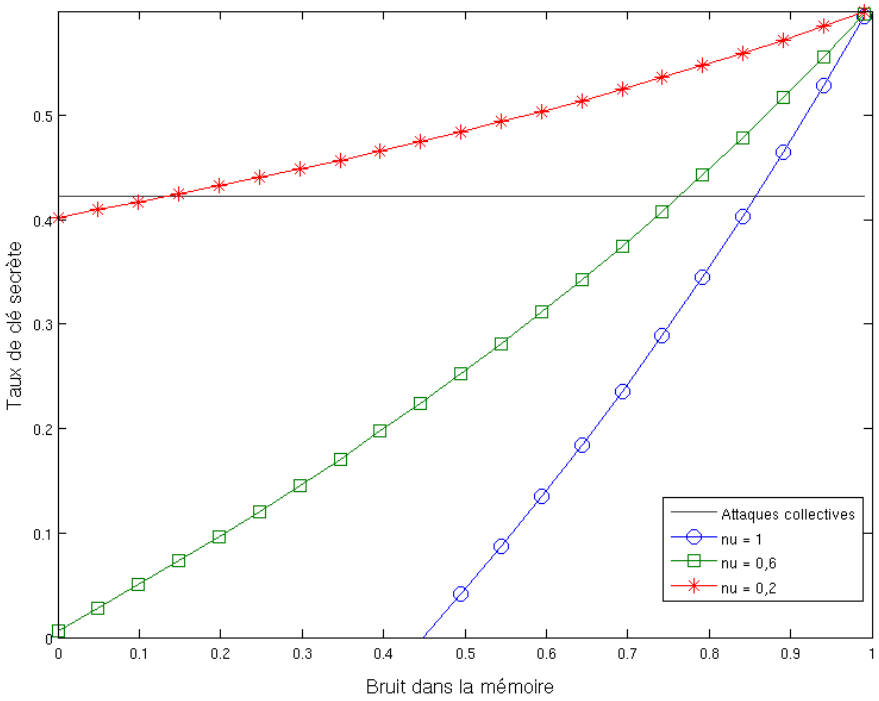


FIGURE 5.13 – Taux de clé secrète pour SARG04 pour trois valeurs de taux de stockage nu et un QBER fixé à 5 % en fonction du bruit p dans la mémoire.

est supérieur à 1 %.

Enfin, une dernière façon d'analyser ces résultats est de calculer le taux de clé secrète pour un QBER fixé à une valeur habituelle rencontrée dans les expériences sur le terrain. On choisit ici la valeur de 5 %. Dans ce cas on peut calculer $t_{\text{coll}} = 0,42$. On a tracé dans la figure 5.13 le taux de clé secrète pour un QBER de 5 % pour trois valeurs de taux de stockage en fonction du bruit p.

On voit sur ce graphe que pour un taux de stockage $\nu = 0,2$ le taux de clé secrète dans le modèle de la mémoire bruitée est supérieur à $t_{\text{coll}} = 0.42$ dès lors que le bruit dans la mémoire p est supérieur à $0,15$.

5.4 Comparaison des protocoles face à ce type d'attaque

Dans cette section nous analysons qualitativement les résultats obtenus dans la section précédente en comparant le QBER critique dans le modèle de la mémoire bruitée pour les trois protocoles de distribution quantique de clés étudiés.

Le QBER critique est un paramètre caractérisant la robustesse d'un protocole dans un modèle de sécurité donné face aux erreurs introduites par le canal quantique entre Alice et Bob. Dans une situation normale, ces erreurs proviennent du bruit électronique, des fausses détections ou d'une mauvaise calibration. Cependant, pour garantir la sécurité du protocole, ces erreurs sont attribuées à l'action de l'espion sur le canal quantique. Les preuves de sécurité présentées dans la section précédentes permettent alors de borner la quantité d'information accessible à l'espion en fonction de ce taux d'erreur. Au delà d'un certain seuil, le QBER critique, le taux de clé secrète s'annule.

Lorsque l'adversaire est limité par le bruit de sa mémoire quantique, les preuves de sécurité présentées dans la section précédente permettent d'accroître la robustesse des 3 protocoles de distribution quantique de clés étudiés sous certaines conditions de bruit ou de taux de stockage. Les valeurs limites pour le taux de stockage ν et le bruit p à partir desquelles le modèle de la mémoire bruitée accroît la robustesse des protocoles sont résumées dans le tableau suivant :

Protocole	pour un taux de stockage fixé $\nu = 1$	pour un bruit fixé $p = 0$
BB84	$p > 0,82$	$\nu < 0,20$
six-states	$p > 0,77$	$\nu < 0,27$
SARG04	$p > 0,76$	$\nu < 0,28$

Ce tableau se lit de la façon suivante : concernant le protocole BB84, pour un taux de stockage fixé à 1, la preuve de sécurité dans le modèle de la mémoire bruitée

présentée dans ce chapitre améliore la borne connue lorsque $p > 0,82$.

Les preuves de sécurité établies dans la section précédente ne sont pas optimales (elles surestiment la puissance de l'espion), c'est pour cela que le domaine de sécurité des protocoles étudiés est étendu par rapport aux preuves existantes pour un domaine (ν, p) donné. Cette situation rend plus difficile la comparaison directe des performances des différents protocoles dans le modèle de la mémoire bruitée : en effet, il est impossible de connaître la "proximité" de notre preuve de sécurité avec la preuve de sécurité optimale et donc de savoir si cette "proximité" est conservée entre les protocoles.

Ainsi, le fait que le domaine de sécurité de SARG04 soit plus étendu que celui de BB84 peut provenir du fait que la preuve de sécurité dans le modèle de la mémoire bruitée est plus proche de la preuve optimale dans le cas de SARG04 qu'elle ne l'est pour BB84. Cela ne signifie pas a priori que la performance de SARG04 s'améliore plus que celle de BB84 lorsque l'adversaire est limité par le bruit de sa mémoire quantique.

Conclusion

Contributions

Les travaux de recherche effectués au cours de cette thèse ont contribué à l'analyse de la sécurité des protocoles de distribution quantique de clé dans des modèles de sécurité où l'espion est limité par la qualité de sa mémoire quantique.

Nous avons présenté un modèle de sécurité pour les protocoles de distribution quantique de clé dans lequel l'adversaire n'a pas accès à une mémoire quantique. Dans ce modèle, nous avons pu paramétrer entièrement les attaques de l'espion : d'une part en considérant l'ensemble des interactions entre le qubit d'Alice et le système quantique de l'espion compatibles avec le taux d'erreur mesuré par Alice et Bob et d'autre part en considérant l'ensemble des POVM utilisables par l'espion pour mesurer ses états quantique. Une optimisation numérique de ces paramètres nous a alors permis d'obtenir des nouvelles bornes de sécurité pour les protocoles six-states et SARG04 dans le modèle des attaques sans mémoire et de confirmer un résultats existant pour le protocole BB84.

En empêchant l'utilisation de mémoire quantique par l'espion, on s'attend à une diminution de la puissance de son attaque sur les protocoles de distribution quantique de clés par rapport aux attaques cohérentes, collectives mais aussi individuelles. La question à laquelle nous avons répondu était de savoir de combien exactement. Nous avons prouvé que le passage d'un adversaire limité aux attaques individuelles à un adversaire sans mémoire quantique augmentait le QBER critique au delà duquel il n'est plus possible de distiller une clé de $14,6$ % à $15,4$ % pour BB84 (un résultat similaire donne un passage de $14,8$ % à $17,5$ % pour SARG04). Pour *six-states*, nous avons prouvé que le gain était encore plus important avec un passage de $15,6$ % à $20,4$ % entre les attaques individuelles et les attaques sans mémoire. Nous avons attribué cette différence assez nette au plus grand nombre de bases possibles de ce protocole qui rendent l'attaque de l'espion moins efficace en l'absence de mémoire lorsque la mesure doit être effectuée avant la phase de réconciliation.

Nous avons ensuite présenté un modèle de sécurité avec un adversaire limité par le bruit de sa mémoire quantique adapté à l'étude de la sécurité des protocoles

de distribution quantique de clé. On pouvait normalement s'attendre à une amélioration des bornes de sécurité existantes quelle que soit la qualité de la mémoire quantique considérée. En effet, une preuve de sécurité optimale dans le modèle de la mémoire bruitée doit naturellement se réduire à la preuve de sécurité contre les attaques cohérentes dans le cas d'une mémoire non bruitée et non bornée. Mais en raison de l'utilisation de bornes non optimales dans notre preuve, nous n'avons pu étendre le domaine de sécurité des trois protocoles de distribution quantique de clés étudiés dans le modèle de la mémoire quantique bruitée que pour un ensemble restreint des valeurs des paramètres caractérisant la mémoire. Ces paramètres permettant de caractériser la qualité et la quantité de la mémoire quantique sont les suivants : le bruit dans la mémoire est défini par un réel p compris entre 0 et 1 et la quantité de mémoire quantique disponible est définie par le taux de stockage ν.

Pour les trois protocoles de distribution quantique de clés étudiés, nous avons prouvé que le domaine de sécurité était étendu lorsque le bruit dans la mémoire quantique de l'espion passait au dessus d'une valeur critique (cette valeur étant similaire pour les trois protocoles étudiés). De même pour une mémoire quantique sans bruit, nous avons prouvé que le domaine de sécurité de ces trois protocoles est étendu lorsque le taux de stockage diminue au delà d'un seuil critique. Ces résultats permettent de calculer précisément une borne supérieure sur l'information mutuelle entre l'espion et les participants honnêtes pour l'ensemble des paramètres de la mémoire quantique. Dans la limite d'une mémoire complètement bruitée ou d'un taux de stockage nul on retrouve les résultats obtenus sur les attaques optimales sans mémoire.

Perspectives

Les résultats obtenus dans cette thèse ont démontré l'utilité de nouveaux modèles de sécurité pour les protocoles de distribution quantique de clés et ont ouvert la voie à de futures recherches dans le domaine. En particulier, nous avons identifié quatre pistes :

- Il s'agirait tout d'abord d'étendre nos recherches à d'autres protocoles de distribution quantique de clé existants. Il serait en particulier intéressant d'étudier le comportement des protocoles de distribution quantique de clés à variables continues dans les modèles d'attaque sans mémoire et avec mémoire quantique bruitée.

- Un sujet que nous n'avons pas eu le temps d'aborder au cours de cette thèse est l'élaboration d'un nouveau protocole de distribution quantique de clé dont le mode de fonctionnement serait particulièrement défavorable à un espion n'ayant pas de mémoire quantique ou ayant accès à une mémoire quantique

bruitée.

- Les preuves de sécurité des protocoles de distribution quantique de clé dans le modèle de la mémoire bruitée peuvent être améliorées. Cela permettrait d'étendre encore plus le domaine de sécurité de ces protocoles et même idéalement de trouver la preuve de sécurité optimale. Une des pistes envisageables est l'utilisation des méthodes développées récemment dans [Berta 2011] et basées sur la capacité quantique de la mémoire plutôt que la capacité classique.

- La qualité de la mémoire quantique de l'espion n'est pas la seule contrainte physique qu'il est possible de lui imposer. Il serait intéressant d'étudier de nouveaux modèles de sécurité dans lesquels la contrainte porterait sur le nombre, la qualité ou le type de portes quantiques réalisables par l'espion.

Annexe A

Code MATLAB pour l'optimisation de l'information mutuelle entre Alice et Eve

Le programme MATLAB présenté ci-après permet d'optimiser la valeur de l'information mutuelle entre Alice et Eve sur l'ensemble des attaques sans mémoire : c'est à dire sur l'ensemble des interactions compatibles avec le taux d'erreur observé par Alice et Bob et sur l'ensemble des POVM utilisés par Eve.

```
%%% Optimisation de l'information mutuelle entre Alice et Eve
%%% pour plusieurs valeurs de QBER pour BB84 dans le modele
%%% de l'attaquant sans memoire

n=20;        % nombre de points a considerer pour
             % le parametre alpha a optimiser dans rho_ABE
m=20;        % nombre de points a considerer pour le QBER

QBER=[0:m]/(4*m);   % on choisit un QBER entre 0 et 1/4
Iae=zeros(1,m+1);   % pour stocker le resultat de
                        % l'optimisation pour chaque QBER

alpha_opti=zeros(1,m+1);     % valeur optimale de
                             % alpha pour chaque QBER
POVM=zeros(16,16,m+1,n);     % POVM optimaux pour
                % chaque valeur de alpha
                % et chaque QBER
M_opti=zeros(16,16,m+1);     % contient les POVM optimaux
                % pour chaque QBER

for i=1:(m+1),  % on fait une boucle sur les valeurs du QBER

    Q=QBER(i);
    Iae_alpha=zeros(1,n);   % vecteur qui contiendra
                % les valeurs de Iae pour
                % chaque valeur de alpha

    for j=1:n,          % on fait une boucle sur les
                %valeurs de alpha
```

```
        alpha=1-2*Q+(j-1)*Q/(n-1);  % on assigne une valeur a alpha

    cvx_begin sdp quiet
        variable M(16,16) symmetric
        maximize(Iae(alpha,Q,M))    % choix de la quantite
                    % a maximiser
        M(1:4,1:4)+M(5:8,5:8)+M(9:12,9:12)
        +M(13:16,13:16)==eye(4)
        M>=0              % on indique ici les
                    % contraintes sur le POVM
    cvx_end

        POVM(:,:,i,j)=M;
        Iae_alpha(1,j)=cvx_optval;
    end

    [Iae(1,i),indice]=max(temp);
    alpha_opti(1,i)=1-2*Q+(indice-1)*Q/(n-1);

        % on obtient dans ces 2 lignes a la fois la
        % valeur de alpha qui maximise Iae et max(Iae)

    M_opti(:,:,i)=POVM(:,:,i,indice);

            % on stocke ici le POVM qui maximise Iae

end

QBER
alpha_opti
Iae         % on affiche ici les resultats

% on trace les informations mutuelles entre Alice et Bob
% d'une part et Alice et Eve d'autre part

plot(QBER,Iae,QBER,Iab(QBER))

% on calcule le QBER pour lequel les 2 courbes se croisent

[null,indice]=min(abs(Iae-Iab(QBER)));
QBER(indice)
```

Le programme MATLAB présenté ci-après permet de calculer la purification $\rho_{ABE} = |\Psi\rangle\langle\Psi|_{ABE}$ de l'état ρ_{AB} en fonction des paramètres de l'attaque sans mémoire quantique α et Q pour le protocole BB84.

```
function out = rhoABE(a,Q)

    % Initialisation des etats de Bell

    fp=[1;0;0;1]/sqrt(2);
    fm=[1;0;0;-1]/sqrt(2);
    pp=[0;1;1;0]/sqrt(2);
    pm=[0;1;-1;0]/sqrt(2);

    % Calcul de la purification rho_ABE de rho_AB

    out = op(sqrta(a)*kron(fp,fp)+sqrta(1-Q-a)*kron(fm,fm)
+sqrta(1-Q-a)*kron(pp,pp)+sqrta(2*Q+a-1)*kron(pm,pm));

end
```

Le programme MATLAB présenté ci-après permet de calculer l'information mutuelle entre Alice et Eve en fonction de tous les paramètres définissant l'attaque sans mémoire quantique d'Eve sur BB84.

```
function out = Iae(a,Q,X)

    rho=rhoABE(a,Q); % calcul de la purification

    % initialisation des operateurs de mesure

    ze=op([1;0]);
    un=op([0;1]);
    pl=op([1;1]/sqrt(2));
    mo=op([1;-1]/sqrt(2));

    ze=kron(ze,eye(2));
    un=kron(un,eye(2));
    pl=kron(pl,eye(2));
    mo=kron(mo,eye(2));

    ze=kron(ze,eye(4));
    un=kron(un,eye(4));
    pl=kron(pl,eye(4));
    mo=kron(mo,eye(4));

    % Calcul des etats de l'espion

    rhoE00=partial_trace(ze*rho,[0,0,1],[2,2,4])/trace(ze*rho);
    rhoE10=partial_trace(un*rho,[0,0,1],[2,2,4])/trace(un*rho);
    rhoE01=partial_trace(pl*rho,[0,0,1],[2,2,4])/trace(pl*rho);
    rhoE11=partial_trace(mo*rho,[0,0,1],[2,2,4])/trace(mo*rho);

    % Initialisation du POVM

    M1=X(1:4,1:4);
```

```
    M2=X(5:8,5:8);
    M3=X(9:12,9:12);
    M4=X(13:16,13:16);

    % Calcul des probabilites des resultats de mesure

    p100=trace(M1*rhoE00);
    p110=trace(M1*rhoE10);
    p101=trace(M1*rhoE01);
    p111=trace(M1*rhoE11);

    p200=trace(M2*rhoE00);
    p210=trace(M2*rhoE10);
    p201=trace(M2*rhoE01);
    p211=trace(M2*rhoE11);

    p300=trace(M3*rhoE00);
    p310=trace(M3*rhoE10);
    p301=trace(M3*rhoE01);
    p311=trace(M3*rhoE11);

    p400=trace(M4*rhoE00);
    p410=trace(M4*rhoE10);
    p401=trace(M4*rhoE01);
    p411=trace(M4*rhoE11);

    % Calcul des entropies conditionelles

    hKXB=(1/4)*(entropy(p100,p200,p300,p400)
+entropy(p101,p201,p301,p401)+entropy(p110,p210,p310,p410)
+entropy(p111,p211,p311,p411));

    hKB=(1/2)*(
entropy((p100+p110)/2,(p200+p210)/2,(p300+p310)/2,(p400+p410)/2)
+entropy((p101+p111)/2,(p201+p211)/2,(p301+p311)/2,(p401+p411)/2));

    % On renvoie la valeur de l'information mutuelle

    out = hKB - hKXB;

end
```

Bibliographie

[Afzelius 2009] Mikael Afzelius, Christoph Simon, Hugues de Riedmatten et Nicolas Gisin. *Multimode quantum memory based on atomic frequency combs.* Phys. Rev. A, vol. 79, page 052329, May 2009. (Cité en page 96.)

[Aharonov 2000] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani et Andrew C. Yao. *Quantum bit escrow.* In Proceedings of the thirty-second annual ACM symposium on Theory of computing, STOC '00, pages 705–714, New York, NY, USA, 2000. ACM. (Cité en page 45.)

[Ballester 2008] M. A. Ballester, S. Wehner et A. Winter. *State Discrimination With Post-Measurement Information.* Information Theory, IEEE Transactions on, vol. 54, no. 9, pages 4183 –4198, sept. 2008. (Cité en page 78.)

[Bechmann-Pasquinucci 1999] H. Bechmann-Pasquinucci et N. Gisin. *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography.* Phys. Rev. A, vol. 59, no. 6, pages 4238–4248, Jun 1999. (Cité en pages 83 et 124.)

[Bechmann-Pasquinucci 2006] H. Bechmann-Pasquinucci. *Eavesdropping without quantum memory.* Phys. Rev. A, vol. 73, no. 4, page 044305, Apr 2006. (Cité en page 73.)

[Bennett 1983] C.H. Bennett, G. Brassard, S. Breidbart et S. Wiesner. *Quantum Cryptography, or Unforgeable Subway Tokens.* In Advances in Cryptography : Proceedings of Crypto 82 Plenum (New York), pages 267–275, 1983. (Cité en page 38.)

[Bennett 1984] Charles Bennett et Gilles Brassard. *Quantum cryptography : Public key distribution and coin tossing.* In IEEE, editeur, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175–179, 1984. (Cité en pages x, xii, 46, 47, 58, 63, 72, 94 et 151.)

[Bennett 1992a] Charles Bennett, François Bessette, Gilles Brassard, Louis Salvail et John Smolin. *Experimental Quantum Cryptography.* Journal of Cryptology, vol. 5, pages 3–28, 1992. (Cité en pages xii, 63 et 72.)

[Bennett 1992b] Charles H. Bennett, Gilles Brassard et N. David Mermin. *Quantum cryptography without Bell's theorem.* Phys. Rev. Lett., vol. 68, no. 5, pages 557–559, Feb 1992. (Cité en pages 62 et 95.)

[Berta 2011] M. Berta, F. Brandao, M. Christandl et S. Wehner. *Entanglement Cost of Quantum Channels.* ArXiv e-prints, 2011. (Cité en page 137.)

[Biham 1997] Eli Biham et Tal Mor. *Security of Quantum Cryptography against Collective Attacks.* Phys. Rev. Lett., vol. 78, pages 2256–2259, Mar 1997. (Cité en page 66.)

[Boller 1991] K.-J. Boller, A. Imamolu et S. E. Harris. *Observation of electromagnetically induced transparency.* Phys. Rev. Lett., vol. 66, no. 20, pages 2593–2596, May 1991. (Cité en page 96.)

[Branciard 2005] Cyril Branciard, Nicolas Gisin, Barbara Kraus et Valerio Scarani. *Security of two quantum cryptography protocols using the same four qubit states*. Phys. Rev. A, vol. 72, no. 3, page 032301, Sep 2005. (Cité en pages 61, 89 et 131.)

[Brassard 1991] G. Brassard et C. Crépeau. *Quantum Bit Commitment and Coin Tossing Protocols*. In in Advances in Cryptology : Proceedings of Crypto '90, Lecture Notes in Computer Science, pages 49–61. Springer-Verlag, 1991. (Cité en page 46.)

[Brassard 1993] Gilles Brassard, Richard Jozsa et Denis Langlois. *A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties*. In Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on, pages 362 –371, 1993. (Cité en pages 46 et 47.)

[Brassard 2000] Gilles Brassard, Norbert Lütkenhaus, Tal Mor et Barry C. Sanders. *Limitations on Practical Quantum Cryptography*. Phys. Rev. Lett., vol. 85, pages 1330–1333, Aug 2000. (Cité en pages 61 et 151.)

[Bruß 1998] Dagmar Bruß. *Optimal Eavesdropping in Quantum Cryptography with Six States*. Phys. Rev. Lett., vol. 81, no. 14, pages 3018–3021, Oct 1998. (Cité en pages 59, 83, 94, 107, 127 et 151.)

[Budker 1999] D. Budker, D. F. Kimball, S. M. Rochester et V. V. Yashchuk. *Nonlinear Magneto-optics and Reduced Group Velocity of Light in Atomic Vapor with Slow Ground State Relaxation*. Phys. Rev. Lett., vol. 83, no. 9, pages 1767–1770, Aug 1999. (Cité en page 96.)

[Cachin 1998] Christian Cachin, Claude Crepeau et Julien Marcil. *Oblivious Transfer with a Memory-Bounded Receiver*, nov 1998. (Cité en pages xi et 48.)

[Canetti 2001] Ran Canetti et Marc Fischlin. Universally Composable Commitments, volume 2139. Janvier 2001. (Cité en page 46.)

[Canetti 2006] Ran Canetti, Eyal Kushilevitz et Yehuda Lindell. *On the Limitations of Universally Composable Two-Party Computation Without Set-Up Assumptions*. Journal of Cryptology, vol. 19, no. 2, pages 135–167, Avril 2006. (Cité en pages x, 45 et 46.)

[Carter 1977] Lawrence J. Carter et Mark N. Wegman. *Universal classes of hash functions*. In Proceedings of the ninth annual ACM symposium on Theory of computing, pages 106–112, 1977. (Cité en pages 45 et 57.)

[Chailloux 2009] A. Chailloux et I. Kerenidis. *Optimal Quantum Strong Coin Flipping*. In Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on, pages 527 –533, oct. 2009. (Cité en page 45.)

[Chefles 2000] Anthony Chefles. *Quantum state discrimination*. Contemporary Physics, vol. 41, no. 6, pages 401–424, 2000. (Cité en page 78.)

[Cirac 2009] J. I. Cirac et R. Renner. *de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography*. Phys. Rev. Lett., vol. 102, no. 11, page 110504, Mar 2009. (Cité en page 56.)

[Cover 2006] Thomas M. Cover et Joy A. Thomas. Elements of Information Theory 2nd Edition. Wiley-Interscience, 2 édition, Juillet 2006. (Cité en page 1.)

[Crepeau 1987] Claude Crepeau. *Equivalence Between Two Flavours of Oblivious Transfers*, 1987. (Cité en page 44.)

[Crépeau 1988] Claude Crépeau et Joe Kilian. *Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract)*. In 29th annual IEEE, pages 42–52, 1988. (Cité en page 46.)

[Crépeau 1994] C. Crépeau. *Quantum Oblivious Transfer*. Journal of Modern Optics, vol. 41, pages 2445–2454, 1994. (Cité en pages x et 48.)

[Csiszar 1978] I. Csiszar et J. Korner. *Broadcast channels with confidential messages*. Information Theory, IEEE Transactions on, vol. 24, no. 3, pages 339 – 348, may 1978. (Cité en pages 64, 65 et 80.)

[Damgaard 2005] Ivan Damgaard, Serge Fehr, Louis Salvail et Christian Schaffner. *Cryptography In the Bounded Quantum-Storage Model*. In Proceedings of the 46th IEEE Symposium on Foundations of Computer Science - FOCS 2005, page 449, 2005. (Cité en page 49.)

[Damgaard 2007] Ivan B. Damgaard, Serge Fehr, Renato Renner, Louis Salvail et Christian Schaffner. *A tight high-order entropic quantum uncertainty relation with applications*. In In Advances in Cryptology—CRYPTO '07, volume 4622 of Lecture Notes in Computer Science, pages 360–378. Springer, 2007. (Cité en pages 53 et 111.)

[Datta 2006] Anupam Datta, Ante Derek, John Mitchell, Ajith Ramanathan et Andre Scedrov. *Games and the Impossibility of Realizable Ideal Functionality*. In Shai Halevi et Tal Rabin, editeurs, Theory of Cryptography, volume 3876 of *Lecture Notes in Computer Science*, chapitre 19, pages 360–379. Springer Berlin / Heidelberg, 2006. (Cité en page 46.)

[Devetak 2005] I. Devetak et A. Winter. *Distillation of secret key and entanglement from quantum states*. Royal Society of London Proceedings Series A, vol. 461, pages 207–235, Janvier 2005. (Cité en page 66.)

[Ding 2007] Yan Zong Ding, Danny Harnik, Alon Rosen et Ronen Shaltiel. *Constant-Round Oblivious Transfer in the Bounded Storage Model*. Journal of Cryptology, vol. 20, pages 165–202, 2007. 10.1007/s00145-006-0438-1. (Cité en page 48.)

[Durt 2010] T. Durt, B.-G. Englert, I. Bengtsson et K. Zyczkowski. *On mutually unbiased bases*. ArXiv e-prints, Avril 2010. (Cité en page 60.)

[Ekert 1991] Artur K. Ekert. *Quantum cryptography based on Bell's theorem*. Phys. Rev. Lett., vol. 67, no. 6, pages 661–663, Aug 1991. (Cité en page 62.)

[Even 1983] Shimon Even. *A protocol for signing contracts*. SIGACT News, vol. 15, no. 1, pages 34–39, 1983. (Cité en page 43.)

[Even 1985] Shimon Even, Oded Goldreich et Abraham Lempel. *A randomized protocol for signing contracts*. Commun. ACM, vol. 28, no. 6, pages 637–647, 1985. (Cité en page 44.)

[Gisin 2002] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel et Hugo Zbinden. *Quantum cryptography.* Reviews of Modern Physics, vol. 74, no. 1, pages 145–195, Mars 2002. (Cité en pages 60, 66, 100, 101, 102, 103 et 105.)

[Gisin 2004] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner et V. Scarani. *Towards practical and fast Quantum Cryptography.* eprint arXiv :quant-ph/0411022, Novembre 2004. (Cité en page 63.)

[Goldreich 1987] Oded Goldreich, Silvio Micali et Avi Wigderson. *How to Solve any Protocol Problem.* In In Proc.of STOC. Springer-Verlag, 1987. (Cité en page 44.)

[Grant 2008] M. Grant et S. Boyd. *Graph implementations for nonsmooth convex programs.* In V. Blondel, S. Boyd et H. Kimura, editeurs, Recent Advances in Learning and Control, Lecture Notes in Control and Information Sciences, pages 95–110. Springer-Verlag Limited, 2008. `http://stanford.edu/~boyd/graph_dcp.html`. (Cité en page 80.)

[Grant 2011] M. Grant et S. Boyd. *CVX : Matlab Software for Disciplined Convex Programming, version 1.21.* `http://cvxr.com/cvx`, Avril 2011. (Cité en page 80.)

[Hajiaghayi 2005] MohammadTaghi Hajiaghayi, Jeong H. Kim, Tom Leighton et Harald Räcke. *Oblivious routing in directed graphs with random demands.* In Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC), pages 193–201, 2005. (Cité en page 45.)

[Helstrom 1969] C. W. Helstrom. *Quantum detection and estimation theory.* J. Stat. Phys., vol. 1(2), pages 231–252, 1969. (Cité en pages 78 et 102.)

[Hughston 1993] L. P. Hughston, R. Jozsa et W. K. Wootters. *A complete classification of quantum ensembles having a given density matrix.* Physics Letters A, vol. 183, pages 14–18, Novembre 1993. (Cité en page 47.)

[Hwang 2003] Won-Young Hwang. *Quantum Key Distribution with High Loss : Toward Global Secure Communication.* Phys. Rev. Lett., vol. 91, page 057901, Aug 2003. (Cité en page 61.)

[Inoue 2002] Kyo Inoue, Edo Waks et Yoshihisa Yamamoto. *Differential Phase Shift Quantum Key Distribution.* Phys. Rev. Lett., vol. 89, no. 3, page 037902, Jun 2002. (Cité en page 63.)

[Julsgaard 2004] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek et E. S. Polzik. *Experimental demonstration of quantum memory for light.* Nature, vol. 432, pages 482–486, Novembre 2004. (Cité en page 96.)

[Kasapi 1995] A. Kasapi, Maneesh Jain, G. Y. Yin et S. E. Harris. *Electromagnetically Induced Transparency : Propagation Dynamics.* Phys. Rev. Lett., vol. 74, no. 13, pages 2447–2450, Mar 1995. (Cité en page 96.)

[Kilian 1988] J. Kilian. *Founding cryptography on oblivious transfer.* In In Proceedings of 20th ACM STOC, pages 20–31, 1988. (Cité en page 44.)

[King 2001] C. King. *Additivity for a class of unital qubit channels*. Mai 2001. (Cité en page 98.)

[Koenig 2008] Robert Koenig, Renato Renner et Christian Schaffner. *The operational meaning of min- and max-entropy*. Juillet 2008. (Cité en page 31.)

[Koenig 2009a] R. Koenig et S. Wehner. *A Strong Converse for Classical Channel Coding Using Entangled Inputs*. Physical Review Letters, vol. 103, no. 7, pages 070504–+, 2009. (Cité en pages 51, 52 et 110.)

[Koenig 2009b] R. Koenig, S. Wehner et J. Wullschleger. *Unconditional security from noisy quantum storage*. ArXiv e-prints, Juin 2009. (Cité en pages 49, 109 et 114.)

[Kraus 2005] B. Kraus, N. Gisin et R. Renner. *Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication*. Phys. Rev. Lett., vol. 95, no. 8, page 080501, Aug 2005. (Cité en pages 67, 76 et 113.)

[Lauritzen 2010] Björn Lauritzen, Jiří Minář, Hugues de Riedmatten, Mikael Afzelius, Nicolas Sangouard, Christoph Simon et Nicolas Gisin. *Telecommunication-Wavelength Solid-State Memory at the Single Photon Level*. Phys. Rev. Lett., vol. 104, no. 8, page 080502, Feb 2010. (Cité en page 94.)

[Lo 1997] Hoi-Kwong Lo et H. F. Chau. *Is Quantum Bit Commitment Really Possible ?* Phys. Rev. Lett., vol. 78, pages 3410–3413, Apr 1997. (Cité en page 47.)

[Lo 2001] H.-K. Lo. *Proof of unconditional security of six-state quantum key distribution scheme*. Quant. Inf. Comp., vol. 1, page 81, 2001. (Cité en pages 83 et 124.)

[Lo 2005] Hoi-Kwong Lo, Xiongfeng Ma et Kai Chen. *Decoy State Quantum Key Distribution*. Phys. Rev. Lett., vol. 94, page 230504, Jun 2005. (Cité en page 61.)

[Lütkenhaus 1996] Norbert Lütkenhaus. *Security against eavesdropping in quantum cryptography*. Phys. Rev. A, vol. 54, no. 1, page 97, Jul 1996. (Cité en pages xii, 72, 73, 82 et 83.)

[Lütkenhaus 1999] Norbert Lütkenhaus. *Estimates for practical quantum cryptography*. Phys. Rev. A, vol. 59, pages 3301–3319, May 1999. (Cité en page 65.)

[Lütkenhaus 2000] Norbert Lütkenhaus. *Security against individual attacks for realistic quantum key distribution*. Phys. Rev. A, vol. 61, page 052304, Apr 2000. (Cité en pages 61 et 151.)

[Lydersen 2010] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar et V. Makarov. *Hacking commercial quantum cryptography systems by tailored bright illumination*. Nature Photonics, vol. 4, pages 686–689, Octobre 2010. (Cité en pages xi et 69.)

[Maurer 1992] Ueli M. Maurer. *Conditionally-Perfect Secrecy and a Provably-Secure Randomized Cipher*. Journal of Cryptology, vol. 5, pages 53–66, 1992. (Cité en page 48.)

[Maurer 1993] Ueli M. Maurer. *Secret Key Agreement by Public Discussion From Common Information*. IEEE Transactions on Information Theory, vol. 39, pages 733–742, 1993. (Cité en page 57.)

[Mayers 1994] Dominic Mayers et Louis Salvail. *Quantum Oblivious Transfer is Secure Against Individual Measurements*. In Proceedings of the Third Workshop on Physics and Computation — PhysComp '94, pages 69–77. IEEE Computer Society Press, 1994. (Cité en pages x et 48.)

[Mayers 1996a] D. Mayers. *The Trouble with Quantum Bit Commitment*. eprint arXiv :quant-ph/9603015, Mars 1996. (Cité en page 47.)

[Mayers 1996b] Dominic Mayers. *Unconditionally secure quantum bit commitment is impossible*. Physical Review Letters, vol. 78, page 3414, 1996. (Cité en page 47.)

[Medeiros 2008] Rex Antonio da Costa Medeiros. *Capacité à Zéro-Erreur des Canaux Quantiques*. HAL Archives ouvertes, 2008. (Cité en page 98.)

[Naor 1999] Moni Naor et Benny Pinkas. *Oblivious Transfer with Adaptive Queries*. In Proc. CRYPTO, Springer LNCS, pages 573–590. Springer-Verlag, 1999. (Cité en page 45.)

[Nielsen 2000] MA Nielsen et IL Chuang. *Quantum Computing and Quantum Information*, 2000. (Cité en pages ix, 1 et 25.)

[Odom 2006] B. Odom, D. Hanneke, B. D'Urso et G. Gabrielse. *New Measurement of the Electron Magnetic Moment Using a One-Electron Quantum Cyclotron*. Phys. Rev. Lett., vol. 97, page 030801, Jul 2006. (Cité en page ix.)

[Pirandola 2008] Stefano Pirandola. *Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution*. International Journal of Quantum Information, vol. 6, page 765, 2008. (Cité en pages 100 et 102.)

[Preskill 2011] John Preskill. *Lecture Notes*. `www.theory.caltech.edu/~preskill/ph229/`, 2011. (Cité en page 12.)

[Rabin 1981] Michael O. Rabin. *How To Exchange Secrets with Oblivious Transfer*. Cryptology ePrint Archive, Report 2005/187, 1981. `http://eprint.iacr.org/`. (Cité en page 44.)

[Renner 2005a] Renato Renner. *Security of Quantum Key Distribution*, 2005. (Cité en pages 28, 55, 68, 83, 113 et 124.)

[Renner 2005b] Renato Renner, Nicolas Gisin et Barbara Kraus. *Information-theoretic security proof for quantum-key-distribution protocols*. Phys. Rev. A, vol. 72, no. 1, page 012332, Jul 2005. (Cité en page 76.)

[Richardson 2008] Tom Richardson et Ruediger Urbanke. Modern coding theory. Cambridge University Press, New York, NY, USA, 2008. (Cité en page 10.)

[Saks 1989] M. Saks. *A robust non cryptographic protocol for collective coin flipping.* SIAM J. Discrete Math., vol. 2(2), pages 240–244, 1989. (Cité en page 45.)

[Scarani 2004] Valerio Scarani, Antonio Acín, Grégoire Ribordy et Nicolas Gisin. *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations.* Phys. Rev. Lett., vol. 92, no. 5, page 057901, Feb 2004. (Cité en pages 60, 88, 94, 129 et 151.)

[Shannon 1948] Claude E. Shannon. *A mathematical theory of Communication.* The Bell system technical journal, vol. 27, pages 379–423, Juillet 1948. (Cité en page 2.)

[Shannon 1949] Claude E. Shannon. *Communication Theory of Secrecy Systems.* The Bell system technical journal, vol. 28, pages 656–715, 1949. (Cité en pages ix et 41.)

[Shor 2000] Peter W. Shor et John Preskill. *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.* Physical Review Letters, vol. 85, page 441, 2000. (Cité en pages 55, 63 et 115.)

[Simon 2010] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup et R. J. Young. *Quantum memories. A Review based on the European Integrated Project Qubit Applications (QAP).* The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics, vol. 58, no. 1, pages 1–22, Mai 2010. (Cité en pages xi et 94.)

[Toh 1999] K. C. Toh, M.J. Todd et R. H. Tütüncü. *SDPT3 - a MATLAB software package for semidefinite programming.* Optimization Methods and Software, vol. 11, pages 545–581, 1999. (Cité en page 80.)

[Tomamichel 2011] Marco Tomamichel et Renato Renner. *Uncertainty Relation for Smooth Entropies.* Phys. Rev. Lett., vol. 106, page 110506, Mar 2011. (Cité en page 116.)

[Vandenberghe 1994] Lieven Vandenberghe et Stephen Boyd. *Semidefinite Programming.* SIAM Review, vol. 38, pages 49–95, 1994. (Cité en page 80.)

[Wegman 1981] M. Wegman. *New hash functions and their use in authentication and set equality.* Journal of Computer and System Sciences, vol. 22, no. 3, pages 265–279, Juin 1981. (Cité en pages 45 et 57.)

[Wehner 2008] Stephanie Wehner, Christian Schaffner et Barbara Terhal. *Cryptography from Noisy Storage.* Physical Review Letters, vol. 100, page 220502, 2008. (Cité en pages xi, 49 et 51.)

[Wiesner 1983] Stephen Wiesner. *Conjugate coding.* SIGACT News, vol. 15, no. 1, pages 78–88, 1983. (Cité en pages ix, 37 et 44.)

[Wolfowitz 1957] J. Wolfowitz. *The coding of messages subject to chance errors.* Illinois J. Math., vol. 1(4), pages 591–606, 1957. (Cité en page 110.)

[Wootters 1982] W. K. Wootters et W. H. Zurek. *A single quantum cannot be cloned.* Nature, vol. 299, no. 5886, pages 802–803, Octobre 1982. (Cité en page 36.)

Liste des Abréviations

BB84	Protocole de distribution quantique de clés à 4 états introduit dans [Bennett 1984]
BSC	Binary Symmetric Channel
COW	Coherent One Way
CPTP	Completely Positive Trace Preserving
DPS	Differential Phase Shift
EB	Entanglement Based : basé sur l'intrication
EIT	Electromagnetically Induced Transparency
iid	indépendantes et identiquement distribuées
MUB	*Mutually Unbiased Bases* ou bases mutuellement non biaisées
P&M	Prepare and Measure : préparation et mesure
PNS	Photon Number Splitting attacks ou attaques par partage du nombre de photons [Brassard 2000][Lütkenhaus 2000]
POVM	Positive Operator-Valued Measurement
QBER	Quantum Bit Error Rate (taux d'erreur quantique)
SARG04	Protocole de distribution quantique de clés à 4 états introduit dans [Scarani 2004]
SDP	Semidefinite Programming
six-states	Protocole de distribution quantique de clés à 6 états introduit dans [Bruß 1998]
WSE	*Weak String Erasure*, une primitive cryptographique.

Table des figures