Université de Montréal

La fuite d'information d'une réalisation quantique de primitives cryptographiques classiques

par
Maxime Beaudry

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures et postdoctorales
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en informatique

Août, 2016

RÉSUMÉ

Nous nous intéressons à la réalisation par états quantiques de primitives cryptographiques classiques. Nous introduisons les concepts de l'avantage et de ϵ-enveloppes. Ensuite, nous démontrons que pour tout état, il existe un état strict-correct dont la différence entre leur fuite d'information est bornée supérieurement. Ce résultat démontre qu'il existe une relation entre la continuité de la fuite d'information et la mesure de dépendance entre les registres quantiques d'Alice et Bob. Par la suite, nous démontrons que si un état exhibe une de deux propriétés, sa fuite d'information est toujours bornée inférieurement par la fuite d'un état strict-correct. Ceci démontre que les résultats de Salvail et al. [26] se généralisent pour des états en général respectant ces propriétés. Finalement, nous analysons numériquement la fuite d'information pour des enveloppes réalisant les primitives 1-2-OT et ROT. Nous trouvons un état correct qui atteint un minimum qui bat la borne inférieure précédemment trouvée par Salvail et al. dans [26].

Mots clés: cryptographie quantique, théorie de l'information, cryptographie, continuité de l'information, intrication, transfert équivoque.

ABSTRACT

The Leakage of Information for Quantum Protocols of Classical Cryptographic Primitives

We are interested in classical cryptographic primitive implemented by quantum states. We introduce the concepts of advantage and ϵ-embedding. Following this, we show that for every state there exist a strict-correct state for which the difference between the leakage of both states is upper bounded. This result shows a relation between the leakage and the measure of dependency of Alice and Bob's quantum registers. We then show that if a state exhibits one of two properties, then its leakage is lower bounded by that of a strict-correct state. This shows that the results of Salvail and al. [26] can be generalized to generic states that satisfy those conditions. Finally, we do a numerical analysis of the leakage of embedding for 1-2-OT and ROT primitives. We find a state that leaks less information than the lower bound previously found by Salvail and al. in [26].

Keywords: Quantum Cryptography, Information Theory, Cryptography, Continuity of Information, Entanglement, Oblivious Transfer.

TABLE DES MATIÈRES

LISTE DES FIGURES

NOTATION

$\lg x$	Logarithme en base 2 de x
$\|x\|$	Taille de la chaîne binaire x
$\in_R$	Pris au hasard parmis
a^*	Conjuguée complexe de a
$\|\psi\rangle$	État pur sous forme de vecteur colonne (ket)
$\langle\psi\|$	Transposé conjuguée du ket (bra)
$\mathcal{H}_A$	Espace d'Hilbert A
$\mathbb{C}^d$	Espace des complex de dimension d (qudit)
$\otimes$	Produit Tensoriel
$\subseteq$	Sous-espace
$\setminus$	Soustraction de sous-espace
$\cup$	Union de sous-espace
$A = (a_{ij})_{ij}$	Matrice avec a_{ij} en position ij
$A = (a_{ii})_i$	Matrice diagonale avec a_{ii} sur la diagonale et 0 ailleurs
$\|\|M\|\|_1$	Norme de trace de M
$\delta(M, N)$	Distance de trace entre M et N
$\perp$	Symbole d'effacement
1-2-OT	Transfert équivoque d'un parmis deux
ROT	Transfert équivoque de Rabin
QHMC	Modèle quantique honnête mais curieux

À ma mère et mon père

REMERCIEMENTS

Je tiens à remercier mon directeur de recherche Louis Salvail pour son aide, son expertise et pour être disponible en tout temps.

Merci également aux membres du Laboratoire d'informatique théorique et quantique pour les conversations constructives qui m'ont encouragé à me perfectionner.

Merci à ma famille et à Audrey-Maude qui, tout au long de mon cheminement, ont cru en moi et m'ont permis de poursuivre un cheminement ardu.

Pour terminer, merci à Louis Salvail et à l'Université de Waterloo par l'entremise du programme Cryptoworks21 pour le soutien financier.

INTRODUCTION

Le calcul multiparties est une branche de la cryptographie qui s'intéresse à la réalisation de tâches par de multiples participants. Certaines de ces tâches sont universelles, c'est-à-dire qu'elles peuvent être utilisées pour réaliser n'importe qu'elle autre tâche du même nombre de participants. En ce sens, certaines sont plus puissantes que d'autres.
Ce mémoire s'intéresse à une notion de puissance pour les primitives cryptographiques classiques dans le monde quantique appelé la fuite d'information. Dans le contexte du calcul multiparties, cette quantité permet de mettre en relation les tâches selon une notion de réductibilité ainsi de les hiérarchiser.

Mise en contexte

La cryptographie permet de communiquer publiquement sans révéler le contenu des messages échangés. Classiquement, la méthode RSA, introduite en 1977 par Rivest, Shamir et Adleman [25], est utilisée dans la plupart des systèmes modernes. Cette méthode, basée sur la difficulté de factorisation, encrypte un message en utilisant une clé publique. Le destinataire du message possède à lui seul la clé qui permet de récupérer le contenu en clair.
L'algorithme de Shor découverte en 1994 [29], [30] permet de factoriser en temps polynomial sur un ordinateur quantique. Michele Mosca [22] estime la probabilité de briser RSA-2048 d'ici 2026 à $1/7$ et d'ici 2031 à $1/2$. Ces estimations s'ajoutent au fait que des groupes de recherche réalisent depuis un certain temps des algorithmes quantiques en laboratoire sur des systèmes physiques (Jones et Mosca [16]). De ce fait, la recherche en cryptographie s'oriente de plus en plus vers des solutions résistantes aux ordinateurs quantiques.
Le premier protocole d'échange de clé publique quantique BB84, publié par Bennett et Brassard en 1984 [3], est le premier exemple d'une tâche cryptographique résistante aux attaques quantiques qui utilise les ordinateurs quantiques. BB84 est un protocole qui

établit une clé secrète entre deux participants où l'adversaire est une tierce partie. Pour le calcul à deux parties, tels que le transfert équivoque et la mise en gage, ce sont les participants qui sont les adversaires. Une attaque quantique implique alors des participants quantiques. L'impossibilité de la mise en gage quantique parfaite a été démontrée en 1997 par Lo et Chau [18] ainsi que par Mayers [19].

Plus récemment, Wolf et Wullschleger [32], [33] se sont intéressés à la question de puissance des tâches cryptographiques à deux parties réalisées classiquement. Dans le but d'établir une quantification de celle-ci, ils ont réussi à démontrer qu'il existe une hiérarchisation des primitives cryptographiques réalisée classiquement. De façon similaire, Salvail, Schaffner et Sotáková [26] apportent une hiérarchisation similaire dans le monde quantique pour les primitives cryptographiques. Leur contribution s'applique à des états particuliers appelés stricts-corrects. La question est restée ouverte à savoir si leurs résultats s'étendent à des états plus généraux. Ce mémoire s'intéresse donc à répondre à cette question et à explorer les réalisations quantiques de primitives cryptographiques classiques.

Contributions

Nous présentons premièrement une extension au modèle de Salvail, Schaffner et Sotáková et démontrons que la fuite d'information est continue selon une mesure de l'information que contient l'état. Ensuite, nous montrons que si un état respecte certaines conditions, alors sa fuite d'information doit être supérieure à celle d'un état strict-correct. Ensuite, les calculs numériques de la fuite d'information pour des réalisations de primitives sont faits. Nous montrons des exemples d'états qui parviennent à fuire moins d'information que la borne inférieure pour les états stricts-corrects trouvée par Salvail et al. [26]. Ce résultat laisse une piste de recherche ouverte pour l'optimisation entre la fuite d'information et l'efficacité pour des participants honnêtes des réalisations quantiques.

Plan

Le chapitre 1 introduit le problème central de ce mémoire dans les modèles classiques et quantiques. Nous survolons aussi les résultats de Wolf et Wullschleger ainsi que de Salvail et al.

Au chapitre 2, les outils de la théorie de l'information sont introduits formellement. Nous débutons par la théorie classique, suivie du formalisme quantique informatique et nous terminons par la théorie de l'information quantique.

Le chapitre 3 fait un retour formel sur les concepts survolés du chapitre 1. Nous introduisons les monotones classiques et quantiques. Ces derniers font le pont avec les contributions de ce mémoire présenté dans le chapitre suivant.

Au chapitre 4, nous démontrons que la fuite d'information est une quantité continue selon la notion de l'avantage. Par la suite, nous présentons deux catégories d'états auxquels les résultats de Salvail et al. s'appliquent. Ceux-ci fuient donc plus d'information que la borne inférieure établie pour les états stricts-corrects.

Finalement, le chapitre 5 étudie numériquement la fuite d'information pour deux primitives importantes. Nous démontrons des exemples d'états qui fuient moins que la borne inférieure mentionnée ci-haut.

CHAPITRE 1

CALCUL MULTIPARTIES

Ce premier chapitre sert d'introduction au problème central à ce mémoire. Nous commençons par introduire les primitives cryptographiques classiques. Par la suite, nous définissons le modèle honnête, mais curieux et sa variation quantique. Finalement, nous ferons une courte introduction aux résultats de Wolf et Wullschleger [32], [33] dans le monde classique et de Salvail et al. [26], dans le monde quantique.

1.1 Primitives cryptographiques classiques

Le calcul multiparties s'intéresse à des tâches cryptographiques accomplies par de multiples participants. Dans ce mémoire, nous nous limiterons à deux participants, soit A, Alice, et B, Bob. Ceux-ci ne sont pas en confiance, mais désirent malgré tout collaborer pour calculer une fonction. Cette fonction représente une primitive classique que l'on note P.

Une primitive est réalisée par un protocole qui permet le calcul local et la communication entre les participants. On s'intéresse à la relation entre les entrées, a et b, et les sorties, x et y, d'Alice et Bob respectivement. On définit maintenant formellement une primitive cryptographique.

Définition 1.1 (Primitive cryptographique)**.** *Une primitive est une fonction non déterministe f qui est modélisée par une boîte $P_{\mathsf{X},\mathsf{Y}}$ qui prend en entrée $a \in \mathcal{A}$ chez Alice et $b \in \mathcal{B}$ chez Bob. Cette boîte produit en sortie $x \in \mathcal{X}$ et $y \in \mathcal{Y}$, où $\mathcal{X}$ et $\mathcal{Y}$ sont les ensembles de sorties possibles chez Alice et Bob respectivement. $P_{\mathsf{X},\mathsf{Y}}$ est définie par la distribution de probabilité entre les entrées et les sorties suivante*

$$P^{a,b}_{\mathsf{X},\mathsf{Y}}(x,y) \coloneqq Pr(f(a,b) = (x,y)). \tag{1.1}$$

Cette définition probabiliste d'une primitive permet d'étudier les relations entre ce qu'Alice et Bob produisent à la fin d'un protocole parfait. X et Y englobent tout ce que les participants produisent étant donné leur entrée. À partir de cette définition, nous introduirons les modèles d'étude de primitives dans les sections suivantes qui contextualisera les travaux des chapitres 4 et 5.

1.2 Modèle HMC

Dans le modèle honnête, mais curieux (HMC), le but principal d'Alice et de Bob est d'accomplir une tâche à deux. Ceci signifie qu'ils accomplissent le protocole de façon correcte et obtiennent x et y selon la distribution de probabilité définie par $P_{\mathsf{X},\mathsf{Y}}$. Malgré l'honnêteté des participants, ils sont curieux à propos de la sortie de leur partenaire et tentent obtenir le maximum d'information sur celle-ci. Étant honnête et curieux, toute stratégie d'Alice et Bob pour maximiser leur information additionnelle doit respecter la correctitude du protocole.

Le modèle HMC modifie la définition d'une primitive. Dans ce modèle, les entrées sont prises aléatoirement et données en sortie aux participants. Les sorties originales, que l'on note X' et Y', sont inchangées. Une primitive dans le modèle HMC est alors un protocole qui représente une distribution de probabilité sur X et Y, où $X = (A, X')$ pour Alice et $Y = (B, Y')$ chez Bob. $P_{\mathsf{X},\mathsf{Y}}$ est défini par

$$P_{\mathsf{X},\mathsf{Y}}(x, y) \coloneqq Pr(X = (a, x'), Y = (b, y')) \tag{1.2}$$

où $a \in_R \mathcal{A}$ et $b \in_R \mathcal{B}$. Dans ce cas-ci, a est pris avec probabilité $1/|\mathcal{A}|$ et b avec probabilité $1/|\mathcal{B}|$.

1.2.1 Monotone

Les travaux de Wolf et Wullschleger [32], [33] démontrent qu'il est possible de classifier les primitives cryptographiques classiques selon leur puissance de calcul. Pour quantifier

celle-ci, ils introduisent des quantités entropiques appelées monotones. Une monotone, suite à l'obtention de x et y par la réalisation d'une primitive, ne peut croître par de la communication sans bruit et du calcul entre Alice et Bob. L'intérêt d'une telle quantité est qu'il est possible de prouver l'impossibilité de réduction d'une primitive à une autre en comparant leurs monotones. Par exemple, si la primitive $P_{\mathsf{X},\mathsf{Y}}$ a une monotone α et que $P_{\mathsf{X}',\mathsf{Y}'}$ a une monotone β, alors la réduction de $P_{\mathsf{X},\mathsf{Y}}$ à $P_{\mathsf{X}',\mathsf{Y}'}$ est impossible avec un seul appel si

$$\alpha < \beta.$$

Le chapitre 3 ira plus en détail et introduira ces quantités formellement.

1.3 Modèle QHMC

Le modèle quantique honnête, mais curieux (QHMC) place Alice et Bob désirant réaliser honnêtement une primitive. Comme dans le cas classique, ils peuvent obtenir de l'information additionnelle à propos de la sortie classique de l'autre participant si cette stratégie produit correctement la bonne sortie de leur côté. Les entrées classiques a et b sont prises uniformément au hasard parmi des ensembles $\mathcal{A}$ et $\mathcal{B}$.

L'extension du modèle survient dans la méthode de réalisation du protocole. Au lieu de permettre du calcul et de la communication classique, nous permettons maintenant toute opération et communication quantique durant le protocole. Celui-ci produit alors un encodage de x et y en superposition dans un état quantique. Alice et Bob doivent, suite à la réception de l'état, mesurer leurs registres pour obtenir x et y selon la distribution de probabilité $P_{\mathsf{X},\mathsf{Y}}(x, y)$. Comme dans le cas classique, X et Y contiennent les entrées de la fonction et les sorties. Tout registre quantique résiduel suite à cette mesure peut être utilisé pour extraire de l'information additionnelle par une stratégie de mesure.

1.3.1 Fuite d'information

Le formalisme quantique sera introduit à la section 2.2 du chapitre 2, mais intuitivement, une stratégie curieuse dans le modèle quantique aurait la forme d'une mesure sur les registres d'un participant. Cette stratégie, pour être honnête, doit produire la bonne sortie ainsi que de l'information additionnelle. Puisqu'un état quantique permet à Alice et à Bob d'être intriqués, la quantité d'information que contient cet état peut être supérieure pour un adversaire malhonnête. Le théorème d'Holevo (théorème 2.4) énonce le fait que toute stratégie de mesure doit produire moins d'information classique que l'information quantique qu'il contient. Nous capturons la différence entre la meilleure stratégie d'un participant malhonnête et la meilleure stratégie d'un participant honnête et nous appelons cette quantité la fuite d'information.

Les travaux de Salvail et al. [26] démontrent que cette quantité agit comme une monotone pour les réalisations quantiques par états stricts-corrects. Un état strict-correct révèle le minimum d'information à des participants honnêtes, ce qui correspond à l'information accessible par une réalisation parfaite de la primitive. Ce mémoire s'intéresse à ce qui arrive lorsque ces résultats sont généralisés pour des réalisations par des états qui peuvent laisser fuire de l'information supplémentaire pour une primitive parfaite même si les participants sont complètement honnêtes.

1.4 Résumé

Dans ce chapitre, les primitives cryptographiques ont étés introduites dans le cadre des modèles HMC et QHMC. De plus, un aperçu des résultats connus a été fait dans le but de contextualiser la recherche de ce mémoire. Les concepts et outils mathématiques nécessaires au développement des résultats sont présentés dans le chapitre suivant.

CHAPITRE 2

THÉORIE DE L'INFORMATION

Ce chapitre introduit les concepts et les outils nécessaires au développement des résultats de ce mémoire. Nous débutons par présenter l'information classique. Ensuite, le formalisme de la mécanique quantique est introduit. Finalement, nous définissons les concepts de la théorie de l'information quantique.

2.1 Information classique

L'article fondateur de Claude Shannon sur l'entropie d'une variable aléatoire [28] présente l'information comme une mesure de l'incertitude que contient une source d'aléa. Le modèle présenté sera une variante présentée dans le livre par Wilde [31] sur la théorie de l'information quantique. Les preuves des théorèmes sont toutes présentes dans ce livre et dans le Nielsen et Chuang [24].

2.1.1 Entropie de Shannon

Soit une variable aléatoire X et ses réalisations x parmi un alphabet $\mathcal{X}$. Chaque réalisation a une probabilité $p_x = P_{\mathsf{X}}(x)$ d'être le résultat d'une expérience. L'entropie de la variable aléatoire X est :

Définition 2.1 (Entropie de Shannons)**.**

$$H(X) = -\sum_{x\in\mathcal{X}} P_{\mathsf{X}}(x) \lg \left(P_{\mathsf{X}}(x)\right). \tag{2.1}$$

Le logarithme est en base 2 et l'entropie est calculée en bits. En théorie de l'information, l'entropie est une mesure d'information. En effet, si on apprend la réalisation x on obtient en moyenne l'information qu'elle contient, soit $\lg\left(p_x\right)$. Pour parler de l'entropie d'une

distribution de probabilité $\{p_x\}_x$, nous noterons $H(\{p_x\}_x)$.

2.1.2 Entropie conjointe

Soit X et Y, deux variables aléatoires sur des alphabets respectifs $\mathcal{X}$ et $\mathcal{Y}$. On peut définir l'entropie conjointe $H(X,Y)$ comme l'incertitude sur une réalisation simultanée de X et Y.

Définition 2.2 (Entropie conjointe)**.** *L'entropie conjointe de deux variables aléatoires X et Y avec distribution conjointe $P_{\mathsf{X},\mathsf{Y}}$ est*

$$H(X,Y) = -\sum_{x,y} P_{\mathsf{X},\mathsf{Y}}(x,y) \lg \left(P_{\mathsf{X},\mathsf{Y}}(x,y)\right). \tag{2.2}$$

Cette quantité peut être considérer comme l'entropie de la variable $Z \equiv (X,Y)$ qui a comme distribution de probabilité $P_{\mathsf{Z}} = P_{\mathsf{X},\mathsf{Y}}$. Notons aussi que si X et Y sont indépendants, alors

$$H(X,Y) = H(X) + H(Y).$$

L'entropie conjointe est additive lorsque les variables sont indépendantes. Il est possible de généraliser cette quantité lorsqu'il y a n variables au lieu de 2. On obtient alors

$$H(X_1, X_2, \cdots, X_n) = -\sum_{x_1,x_2,\cdots,x_n} P_{\mathsf{X}_1,\mathsf{X}_2,\cdots,\mathsf{X}_\mathsf{N}}(x_1, x_2, \cdots, x_n) \cdot \lg \left(P_{\mathsf{X}_1,\mathsf{X}_2,\cdots,\mathsf{X}_\mathsf{N}}(x_1, x_2, \cdots, x_n)\right). \tag{2.3}$$

2.1.3 Entropie conditionnelle

L'information peut aussi être quantifiée par rapport à la connaissance d'un résultat partiel de l'expérience aléatoire. En d'autres mots, nous voulons quantifier le montant d'incertitude sur une variable Y étant donné que nous connaissons la valeur de X.

Définition 2.3 (Entropie conditionnelle)**.** *Soit deux variables aléatoires X et Y avec dis-*

tribution conjointe $P_{\mathsf{X},\mathsf{Y}}$. L'entropie conditionnelle de Y conditionnée sur X est donnée par

$$H(Y|X) = -\sum_{x,y} P_{\mathsf{X},\mathsf{Y}}(x,y) \lg \left(\frac{P_{\mathsf{X},\mathsf{Y}}(x,y)}{P_{\mathsf{X}}(x)} \right). \tag{2.4}$$

Si X et Y sont mutuellement indépendant, alors

$$H(Y|X) = H(Y).$$

Si X et Y sont indépendants, l'entropie conditionnelle est équivalente à l'entropie de Shannon de Y. Nous pouvons mettre en relation les différentes quantités entropiques vues jusqu'à maintenant :

$$H(Y|X) = H(X,Y) - H(X).$$

L'information que X révèle en moyenne sur Y est la différence entre l'information conjointe des deux variables moins l'information que X contient.

2.1.4 Information mutuelle

L'information que X contient sur Y est appelée information mutuelle. En cryptographie, cette quantité est très importante, car elle permet de calculer combien d'information un participant ayant X peut déduire à propos de Y. Définissons cette quantité ci-dessous.

Définition 2.4 (Information mutuelle)**.** *L'information mutuelle $I(X;Y)$ que Y a à propos de X est l'entropie $H(X)$ moins l'entropie conditionnelle $H(X|Y)$,*

$$I(X;Y) = H(X) - H(X|Y). \tag{2.5}$$

Si X et Y sont indépendants, alors $H(X|Y) = H(X)$ et $I(X;Y) = 0$. D'un autre côté, si $H(X|Y) = 0$ (X peut être complètement déterminé par Y) alors $I(X;Y) = H(X)$.

L'information mutuelle est symétrique, c'est-à-dire

$$I(X;Y) = I(Y;X).$$

Ainsi, on peut interpréter l'information mutuelle comme la quantité d'information qui, en moyenne, est partagée entre X et Y. Si Alice et Bob reçoivent respectivement X et Y à la fin d'un protocole, alors ils partagent $I(X;Y)$ bits d'information. Si X et Y sont mutuellement dépendant, ils auront toujours de l'information non nulle à propos de ce que leur partenaire possède comme variable. Ceci étant dit, regardons un exemple avec une distribution de probabilité qui sera utile dans le chapitre 5.

Exemple 2.1. *En 1981, Rabin [20] démontre comment échanger des messages secrets par transfert équivoque. Par la suite, une différente saveur de cette primitive appelée le transfert équivoque d'un parmi deux (1-2-OT) fut développée par Even, Goldreich et Lempel [12]. L'intérêt de recherche de cette primitive a explosé lorsque, en 1988, Kilian [17] démontre qu'elle est complète pour le calcul à deux parties. Toute primitive à deux participants peut être réalisée avec celle-ci et des opérations additionnelles en temps polynomial. Considérons alors la distribution de 1-2-OT dans le modèle honnête mais curieux. Alice reçoit* $x_0, x_1 \in \{0,1\}$ *et Bob* $s, y \in \{0,1\}$.

$$P^{OT}_{\mathsf{X},\mathsf{Y}}((x_0,x_1),(s,y)) = \begin{cases} \frac{1}{8} & \textit{si } y = x_s \\ 0 & \textit{sinon}. \end{cases}$$

Cette distribution décrit l'envoi par Alice de deux bits x_0 *et* x_1*. Bob reçoit avec probabilité* 0.5 x_0 *ou* x_1 *(on écrit donc* $y = x_s$*). Bob n'obtient pas d'information additionnelle sur l'autre message d'Alice (*$x_{\bar{s}}$*) et Alice n'obtient pas d'information additionnelle sur*

s. L'information qui est partagée entre Alice et Bob pour cette distribution est

$$\begin{aligned} I((x_0,x_1);(s,y)) &= H((x_0,x_1)) + H((s,y)) - H((x_0,x_1),(s,y)) \\ &= H\left(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4}\right) + H\left(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4}\right) - H\left(\frac{1}{8},\frac{1}{8},\frac{1}{8},\cdots,\frac{1}{8}\right) \\ &= 2+2-3 \\ &= 1. \end{aligned}$$

Bob connait le bit x_s alors que l'autre lui est inconnu, soit 1 bit d'incertitude. Puisque l'information mutuelle est symétrique, Alice a donc également une incertitude de 1 bit en moyenne sur (s,y). Nous étudierons les deux saveurs de transfert équivoque, celui de Rabin et 1-2-OT, au chapitre 5.

Le théorème suivant est fondamental en théorie de l'information ; l'information mutuelle classique est toujours positive.

Théorème 2.1. *Pour toute variable X et Y, l'information mutuelle entre les deux est toujours au moins 0.*

$$I(X;Y) \geq 0 \tag{2.6}$$

Corollaire 2.1. *L'entropie de X est toujours plus grande (ou égale) à l'entropie de X conditionnée sur Y.*

$$H(X) \geq H(X|Y) \tag{2.7}$$

Ce dernier est une conséquence du théorème précédent et par la définition de l'information mutuelle en (2.5).

2.1.5 Résumé

Dans cette section, l'information d'une variable aléatoire X a été définie par l'entropie $H(X)$. Celle-ci est une fonction de la distribution de probabilité et quantifie l'incertitude sur la valeur que prend X. Nous avons également introduit l'entropie conjointe d'un

ensemble de variables aléatoires. De plus, l'incertitude a aussi été définie dans le contexte où l'on possède une information partielle Y sur la variable X. Celle-ci est quantifiée par l'entropie conditionnelle $H(X|Y)$. Finalement, l'information qui est partagée entre deux variables, $I(X;Y)$, a été introduite et quantifiée dans l'exemple avec la primitive 1-2-OT.

2.2 Formalisme quantique

Dans cette section, le formalisme de la mécanique quantique sera introduit. Le livre sur l'informatique quantique «*Quantum Computing and Quantum Information*» par M.A. Chuang et I.L.Chuang [24] ainsi que le livre «*Quantum Information Theory*» de M.Wilde [31] traitent des sujets qui seront introduits dans cette section. Comme à la section précédente, nous ne prouverons pas les théorèmes, car les preuves se trouvent dans ces livres.

2.2.1 État pur

Débutons par introduire les états quantiques dans un environnement sans bruit. Les systèmes en mécanique quantique peuvent être en superposition d'états classiques. Un exemple informatique serait le bit quantique (qubit) qui peut prendre à la fois la valeur 0 et 1. Contrairement à une variable aléatoire, c'est seulement après l'observation de sa valeur que le qubit prend une valeur définitive. Dans notre formalisme, ce concept est modélisé par un vecteur vivant dans un espace d'Hilbert.

Définition 2.5 (État pur)**.** *L'état d'un système $\mathcal{A}$ est représenté par un vecteur colonne, $|u\rangle_{\mathcal{A}}$, qui vit dans un espace d'Hilbert noté $\mathcal{H}_{\mathcal{A}}$.*

La transposée conjuguée du vecteur $|u\rangle$, notée $\langle u|$, est un état pur sous forme de vecteur rangé dont les composantes sont conjuguées. On définit le produit scalaire entre deux états de la façon suivante.

Définition 2.6 (Produit scalaire)**.** *Le produit scalaire pour deux états quantiques $|u\rangle$ et*

$|v\rangle$ *vivant dans le même espace d'Hilbert* $\mathcal{H}$ *est défini par*

$$\langle u|v\rangle = v_1u_1^* + v_2u_2^* + \cdots + v_nu_n^* \tag{2.8}$$

En informatique quantique, les systèmes sont habituellement des qubits qui vivent dans $\mathbb{C}^2$. Ceux-ci sont de la forme :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.9}$$

avec la condition que

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.10}$$

la norme est 1. L'équation (2.9) représente la notion de superposition ; le qubit $|\psi\rangle$ est en superposition entre 0 et 1 avec amplitude α et β respectivement.

2.2.2 Système composé

Il est possible de généraliser l'équation (2.9) pour un système à plusieurs qubits. Pour cela, il faut introduire un opérateur de l'algèbre linéaire : le produit tensoriel $\otimes$.

Définition 2.7 (Produit tensoriel)**.** *Le produit tensoriel est une fonction qui prend deux matrices* $A = (a_{ij})_{i,j}$ *et* $B = (b_{kl})_{k,l}$ *et produit*

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{bmatrix} \tag{2.11}$$

Exemple 2.2. *Prenons des qubits,* $|v\rangle, |u\rangle \in \mathbb{C}^2$*. Alors,*

$$|k\rangle = |v\rangle \otimes |u\rangle = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \otimes \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} v_1u_1 \\ v_1u_2 \\ v_2u_1 \\ v_2u_2 \end{bmatrix}$$

Avec le produit tensoriel, on peut exprimer un état quantique composé sur plusieurs systèmes. Pour les distinguer, on note en suffixe le nom des espaces d'Hilbert. Pour alléger la notation, on note $|0\rangle_{\mathcal{A}_1} \otimes |0\rangle_{\mathcal{A}_2} \equiv |00\rangle_{\mathcal{A}_1\mathcal{A}_2}$ et de même pour $|01\rangle_{\mathcal{A}_1\mathcal{A}_2}$, $|10\rangle_{\mathcal{A}_1\mathcal{A}_2}$ et $|11\rangle_{\mathcal{A}_1\mathcal{A}_2}$. Analogue à l'équation (2.9), un état à deux qubits est de la forme

$$|\phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

avec la condition de normalisation

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

Le produit tensoriel respecte les propriétés suivantes :

1. Soit un scalaire z et $|u\rangle, |v\rangle$, deux vecteurs, alors :

$$z(|u\rangle \otimes |v\rangle) = (z|u\rangle) \otimes |v\rangle = |u\rangle \otimes (z|v\rangle).$$

2. Pour des vecteurs $|u_1\rangle, |u_2\rangle \in \mathcal{H}_A$ et $|v\rangle \in \mathcal{H}_B$,

$$(|u_1\rangle + |u_2\rangle) \otimes |v\rangle = |u_1\rangle \otimes |v\rangle + |u_2\rangle \otimes |v\rangle.$$

3. Pour des vecteurs $|u\rangle \in \mathcal{H}_A$ et $|v_1\rangle, |v_2\rangle \in \mathcal{H}_B$,

$$|u\rangle \otimes (|v_1\rangle + |v_2\rangle) = |u\rangle \otimes |v_1\rangle + |u\rangle \otimes |v_2\rangle.$$

Dans le langage informatique, un espace d'Hilbert $\mathcal{H}_\mathcal{A}$ est appelé un registre quantique $\mathcal{A}$. De plus, nous utiliserons la notation des ensembles pour dénoter des sous-espaces. Par exemple, prenons un état $|\psi\rangle_\mathcal{A}$ qui est composé de deux qubits. Alors, le qubit 1 vit sur le sous-espace $\mathcal{A}_1 \subseteq \mathcal{A}$ et le qubit 2 vit sur $\mathcal{A}_2 \subseteq \mathcal{A}$. Nous écrirons aussi $\mathcal{A}_2 = \mathcal{A} \backslash \mathcal{A}_1$ et $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2$.

L'intrication est un phénomène qui n'a pas d'analogue classique. Il se manifeste entre deux registres quantiques lorsque l'état conjoint $|\psi\rangle_{\mathcal{AB}}$ ne peut s'exprimer comme produit tensoriel entre un état dans le registre $\mathcal{A}$ et un autre dans le registre $\mathcal{B}$. En d'autres mots,

$$|\psi\rangle_{\mathcal{AB}} \neq |\phi\rangle_{\mathcal{A}} \otimes |\theta\rangle_{\mathcal{B}} \quad \forall |\phi\rangle_{\mathcal{A}}, |\theta\rangle_{\mathcal{B}}$$

est un état intriqué entre $\mathcal{A}$ et $\mathcal{B}$. Voyons un exemple important d'états intriqués.

Exemple 2.3. *Alice et Bob partagent un des états de Bell [2],*

$$\begin{aligned}
\left|\Phi^+\right\rangle_{\mathcal{AB}} &= \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{AB}} + |11\rangle_{\mathcal{AB}}) \\
\left|\Phi^-\right\rangle_{\mathcal{AB}} &= \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{AB}} - |11\rangle_{\mathcal{AB}}) \\
\left|\Psi^+\right\rangle_{\mathcal{AB}} &= \frac{1}{\sqrt{2}}(|01\rangle_{\mathcal{AB}} + |10\rangle_{\mathcal{AB}}) \\
\left|\Psi^-\right\rangle_{\mathcal{AB}} &= \frac{1}{\sqrt{2}}(|01\rangle_{\mathcal{AB}} - |10\rangle_{\mathcal{AB}}).
\end{aligned}$$

Ne pouvant s'exprimer comme un produit d'états distinct chez Alice et Bob, ils sont tous intriqués. Ces états sont extrêmement importants dans le domaine de l'informatique (Bennet et al. [4]), la théorie de l'information (Horodecki et al. [15]) et la cryptographie quantique (Ekert [11]). Ils seront aussi utilisés dans l'analyse numérique au chapitre 5.

Pour terminer cette section, énonçons le théorème de Schmidt qui nous permet de décomposer tout état pur biparti en somme sur un indice d'états sur les registres respectifs.

Théorème 2.2. *Pour tout état pur biparti $|\psi\rangle_{\mathcal{AB}}$, où la dimension de $\mathcal{A}$ et $\mathcal{B}$ est la même (d), il existe une base orthonormée $\{|i\rangle_{\mathcal{A}}\}$ sur $\mathcal{A}$ et $\{|i\rangle_{\mathcal{B}}\}$ sur $\mathcal{B}$ tel que l'état s'exprime comme*

$$|\psi\rangle_{\mathcal{AB}} = \sum_{i=0}^{d-1} \sqrt{\lambda_i} |i\rangle_{\mathcal{A}} |i\rangle_{\mathcal{B}} \tag{2.12}$$

où $\sum_i \lambda_i = 1$.

2.2.3 Évolution unitaire

Tout état quantique pur dans un système fermé doit évoluer selon l'équation de Schrödinger [27]. Dans notre formalisme, ceci équivaut à des processus réversibles. Une évolution est donc une matrice unitaire.

Définition 2.8 (Matrice unitaire)**.** *Une matrice unitaire $U = (u_{ij})_{ij}$ est une matrice avec la propriété que*

$$UU^\dagger = U^\dagger U = \mathbb{1} \tag{2.13}$$

avec $U^\dagger = (u^*_{ji})_{i,j}$, la transposée conjuguée de U et $\mathbb{1}$ l'identité.

Ainsi, si l'on applique une transformation sur un système dans l'état $|\psi\rangle$, on a l'état

$$|\psi'\rangle = U|\psi\rangle.$$

Puisque U doit être unitaire, il existe un inverse $U^\dagger$ tel que si on l'applique à l'état ci-haut on obtient

$$U^\dagger|\psi'\rangle = U^\dagger U|\psi\rangle = \mathbb{1}|\psi\rangle = |\psi\rangle,$$

l'état initial. Toute transformation décrite par une matrice unitaire a donc une évolution inverse, soit $U^\dagger$. Deux transformations indépendantes sur deux qubits peuvent s'exprimer par le produit tensoriel. Soit une transformation U_1 agissant sur un registre $\mathcal{A}$ et U_2 sur le registre $\mathcal{B}$. Alors, la matrice unitaire $V = U_1 \otimes U_2$ décrit la transformation simultanée sur $\mathcal{A}$ et $\mathcal{B}$. Il existe des transformations, par contre, qui agissent sur deux qubits de façon simultanée qui ne s'exprime pas comme un produit tensoriel. Par exemple, la transformation du non contrôlé est la transformation suivante

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

et ne peut s'exprimer comme un produit tensoriel de deux matrices unitaires.

2.2.4 États mixtes

Nous avons vu les états purs et les évolutions unitaires dans les sections précédentes. Qu'arrive-t-il lorsqu'on produit une distribution de probabilité sur un ensemble d'états purs ? Les états mixtes serviront de généralisation aux états purs.

Disons qu'Alice produit l'état $|\psi_i\rangle$ avec probabilité p_i. Elle envoie ensuite le résultat, sans révéler i, à Bob. Du point de vue de celui-ci, cet état n'est pas en superposition sur les $|\psi_i\rangle$, mais bien un mélange statistique d'états purs, $\{p_i, |\psi_i\rangle\}_i$. Au lieu de décrire cet état par un vecteur, on utilise plutôt sa matrice densité

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

pour représenter le manque d'information de Bob.

Introduisons maintenant la trace d'une matrice.

Définition 2.9 (Trace)**.** *La trace de la matrice $A = (a_{ij})_{i,j}$ est la somme des éléments sur la diagonale, c'est-à-dire*

$$\mathrm{tr}\,(A) = \sum_i a_{ii}.$$

Toute matrice densité a une trace de 1 et admet une décomposition spectrale

$$\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|. \tag{2.14}$$

Les λ_i ci-haut sont les valeurs propres de ρ et les $|\psi_i\rangle$ sont les vecteurs propres associés. Ils représentent la probabilité que ρ soit réellement dans l'état pur $|\psi_i\rangle$. Cette interprétation provient du fait que les λ_i forment une distribution de probabilité sur l'indice i.

Un état mixte, comme un état pur, peut être intriqué si

$$\rho_{\mathcal{AB}} \neq \sigma_{\mathcal{A}} \otimes \tau_{\mathcal{B}}, \quad \forall \sigma_{\mathcal{A}}, \tau_{\mathcal{B}}.$$

L'évolution des états mixtes se fait également par des matrices unitaires et l'état résultant

d'une transformation U est

$$\rho' = U\rho U^\dagger.$$

La trace partielle est un outil qui permet de passer d'un état conjoint, $\rho_{\mathcal{AB}}$, à l'état local du registre $\mathcal{A}$ ou $\mathcal{B}$.

Définition 2.10 (Trace partielle)**.** *La trace partielle sur le registre $\mathcal{A}$ de l'état $|\psi\rangle\langle\psi|_{\mathcal{A}} \otimes |\phi\rangle\langle\phi|_{\mathcal{B}}$ est*

$$\mathrm{tr}_{\mathcal{A}}\left(|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|\right) = |\phi\rangle\langle\phi|_{\mathcal{B}} \,\mathrm{tr}\left(|\psi\rangle\langle\psi|_{\mathcal{A}}\right). \tag{2.15}$$

L'équation (2.15) ainsi que la linéarité de la trace nous permettent de calculer les états locaux de systèmes intriqués. Voyons un exemple avec un des états de Bell.

Exemple 2.4. *Soit $|\Phi^+\rangle_{\mathcal{AB}} = \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{AB}} + |11\rangle_{\mathcal{AB}})$ partagé entre Alice et Bob. Si l'on trace sur la partie d'Alice,*

$$\begin{aligned}
\mathrm{tr}_{\mathcal{A}}\left(|\Phi^+\rangle\langle\Phi^+|_{\mathcal{AB}}\right) &= \mathrm{tr}_{\mathcal{A}}\left(\frac{1}{2}(|00\rangle_{\mathcal{AB}} + |11\rangle_{\mathcal{AB}})(\langle 00|_{\mathcal{AB}} + \langle 11|_{\mathcal{AB}})\right) \\
&= \frac{1}{2}(|0\rangle\langle 0|_{\mathcal{B}} \,\mathrm{tr}\left(|0\rangle\langle 0|_{\mathcal{A}}\right) + |0\rangle\langle 1|_{\mathcal{B}} \,\mathrm{tr}\left(|0\rangle\langle 1|_{\mathcal{A}}\right) + |1\rangle\langle 0|_{\mathcal{B}} \,\mathrm{tr}\left(|1\rangle\langle 0|_{\mathcal{A}}\right) \\
&\qquad + |1\rangle\langle 1|_{\mathcal{B}} \,\mathrm{tr}\left(|1\rangle\langle 1|_{\mathcal{A}}\right)) \\
&= \frac{1}{2}(|0\rangle\langle 0|_{\mathcal{B}} + |1\rangle\langle 1|_{\mathcal{B}})
\end{aligned}$$

puisque $\mathrm{tr}(|0\rangle\langle 1|) = \mathrm{tr}(|1\rangle\langle 0|) = 0$ *et* $\mathrm{tr}(|0\rangle\langle 0|) = \mathrm{tr}(|1\rangle\langle 1|) = 1$. *L'état local de Bob est un bit classique aléatoire uniforme.*

Pour terminer, il existe une façon alternative de calculer la trace partielle. Soit $\rho_{\mathcal{AB}}$ et une base orthonormée $\{|e_i\rangle\}_i$ de $\mathcal{B}$. La trace sur $\mathcal{B}$ de $\rho_{\mathcal{AB}}$ est

$$\mathrm{tr}_{\mathcal{B}}\left(\rho_{\mathcal{AB}}\right) = \sum_i \langle e_i|_{\mathcal{B}} \rho_{\mathcal{AB}} |e_i\rangle_{\mathcal{B}}. \tag{2.16}$$

Le produit scalaire partiel dans l'équation (2.16) est un abus de notation. Le produit se

fait seulement entre les éléments du registre $\mathcal{B}$. Plus formellement,

$$\langle S|_{\mathcal{AB}}|x\rangle_{\mathcal{B}}$$

est un raccourci pour

$$\langle S|_{\mathcal{AB}}(\mathbb{1}_{\mathcal{A}} \otimes |x\rangle_{\mathcal{B}}).$$

2.2.5 Mesure d'un état

En mécanique quantique, une mesure est un ensemble d'opérateurs qui décrivent chacun un observable. On appelle cet ensemble un POVM (*angl. Positive-Operator Valued Measurement*) et il représente la façon la plus générale de mesurer un état quantique.

Définition 2.11 (POVM)**.** *Un POVM est un ensemble d'opérateurs $\{M_i\}_i$ où chaque opérateur représente l'observable i de la mesure. Les M_i sont tels que*

$$\sum_i M_i^\dagger M_i = \mathbb{1}. \tag{2.17}$$

Une telle mesure, appliqué à l'état ρ donne le résultat i avec la probabilité

$$p(i) \equiv \mathrm{tr}\left(M_i^\dagger M_i \rho\right) \tag{2.18}$$

et l'état résultant de la mesure, si i est connu, est

$$\rho_i' = \frac{M_i \rho M_i^\dagger}{p(i)} = \frac{M_i \rho M_i^\dagger}{\mathrm{tr}\left(M_i^\dagger M_i \rho\right)}. \tag{2.19}$$

Si, par contre, le résultat i n'est pas connu, l'état est une moyenne sur les ρ_i'.

$$\rho' = \sum_i p(i)\rho_i' = \sum_i M_i \rho M_i^\dagger. \tag{2.20}$$

Un cas spécial de POVM est lorsque l'ensemble contient uniquement des projecteurs.

Un projecteur P est une matrice avec la propriété que $P^2 = P$. Une telle mesure est appelée mesure de Von Neumann (ou, alternativement, projective).

Définition 2.12 (Mesure de Von Neumann)**.** *Une mesure de Von Neumann est un POVM où les opérateurs sont des projecteurs P_i. La probabilité d'observer i est*

$$p(i) \equiv \mathrm{tr}\left(P_i \rho\right)$$

et l'état résultant, si i est connu, est

$$\rho_i' = \frac{P_i \rho P_i}{\mathrm{tr}\left(P_i \rho\right)}.$$

Une mesure projective est donc un cas spécial de mesure généralisée où les opérateurs ont une forme $P_i = |\psi_i\rangle\langle\psi_i|$ et les $|\psi_i\rangle$ forment une base orthonormée sur l'espace d'Hilbert à mesurer. Un exemple de base est la base calculatoire, c'est-à-dire $\{|x\rangle\}_{x\in\{0,1\}^d}$, les chaînes de bit de longueur d.

2.2.6 Purification

Les états mixtes sont le produit de processus aléatoires, tels que l'envoi d'un état parmi un ensemble $\{|x\rangle\}_{x\in\mathcal{X}}$ avec probabilité p_x. La trace partielle d'un système intriqué (voir Ex. 2.4) produit également un état mixte. Prenons $\rho_{\mathcal{A}}$ et sa décomposition spectrale

$$\rho_{\mathcal{A}} = \sum_x p_x |x\rangle\langle x|_{\mathcal{A}},$$

où $\{|x\rangle\}_x$ est une base orthonormée. On peut interpréter cet état comme étant le mélange statistique $\{p_x, |x\rangle\}$ ou, alternativement, comme la trace partielle de la purification de $\rho_{\mathcal{A}}$. Définissons premièrement ce qu'est une purification.

Définition 2.13 (Purification)**.** *Une purification de $\rho_{\mathcal{A}}$ est un état pur biparti $|\psi\rangle_{\mathcal{AR}}$ sur*

$\mathcal{A}$ et $\mathcal{R}$. L'état a la propriété que

$$\rho_{\mathcal{A}} = \mathrm{tr}_{\mathcal{R}} \left(|\psi\rangle\langle\psi|_{\mathcal{AR}} \right). \tag{2.21}$$

On appelle $\mathcal{R}$ le registre de purification.

En cryptographie quantique, les purifications permettent de considérer les processus aléatoires comme la trace partielle d'un état pur. Tous les états mixtes admettent une purification non unique. Pour $\rho_{\mathcal{A}}$ sous sa forme spectrale $\sum_x p_x |x\rangle\langle x|_{\mathcal{A}}$, on construit

$$|\psi\rangle_{\mathcal{AR}} = \sum_x \sqrt{p_x} |x\rangle_{\mathcal{A}} |x\rangle_{\mathcal{R}}. \tag{2.22}$$

Tracer sur $\mathcal{R}$ donne $\rho_{\mathcal{A}}$ tel que requis par la définition.

2.2.7 Évolution bruitée

Une évolution bruitée, qu'on dénote $T(\rho)$, est une évolution qui produit un état mixte. Toute évolution $T(\rho)$ aura la forme

$$T(\rho) = \sum_i E_i \rho E_i^\dagger$$

où les E_i sont des isométries. Nous appelons ceci la représentation opérateur-somme et les E_i satisfont la propriété de complétude, soit

$$\sum_i E_i^\dagger E_i = \mathbb{1}.$$

Exemple 2.5. *La trace partielle est une évolution bruitée. En effet, soit $\rho_{\mathcal{AB}}$ et une base orthonormée $\{|x\rangle\}_x$ sur $\mathcal{B}$. Alors,*

$$E_x = \langle x|$$

appliqué à l'état donne

$$\begin{aligned} T(\rho_{\mathcal{AB}}) &= \sum_x \langle x|\rho_{\mathcal{AB}}|x\rangle \\ &= \mathrm{tr}_{\mathcal{B}}\left(\rho_{\mathcal{AB}}\right). \end{aligned}$$

Cette dernière égalité vient de (2.16). La trace partielle est donc associée aux opérateurs sommes de la forme $E_i = |\psi_i\rangle$ où $|\psi_i\rangle$ est une base orthonormée sur l'espace à tracer.

Puisque certaines évolutions bruitées peuvent altérer la structure d'un registre (ex. la trace partielle), nous noterons en suffixe le registre de départ et le registre final. Par exemple, une évolution $T(\cdot)$ traçant partiellement sur la partie $\mathcal{B}_2$ d'un registre $\mathcal{B} = \mathcal{B}_1\mathcal{B}_2$ sera notée $T^{\mathcal{B}\to\mathcal{B}_1}(\cdot)$. Cette notation permet de mettre en évidence la structure des registres d'entrée et de sortie.

2.2.8 Mesure de distance

Puisque les états quantiques vivent dans un espace vectoriel, on peut construire des mesures de distance à partir d'une norme donnée. Nous utiliserons la norme de trace.

Définition 2.14 (Norme de Trace)**.** *La norme de trace, autrement dit la l_1-norme, d'un opérateur H est*

$$||H||_1 \equiv \mathrm{tr}\left(\sqrt{H^\dagger H}\right). \tag{2.23}$$

La distance de trace est construite à partir de la norme de trace de la façon suivante :

Définition 2.15 (Distance de Trace)**.** *La distance de trace $\delta(\cdot,\cdot)$ entre deux états ρ et σ est la norme de trace de leur différence. En d'autres mots,*

$$\delta(\rho,\sigma) \equiv \frac{1}{2}||\rho-\sigma||_1. \tag{2.24}$$

Énonçons quelques propriétés de la distance de trace qui seront nécessaires dans les chapitres suivants. La distance de trace est bornée : $0 \leq \delta(\rho,\sigma) \leq 1$. L'égalité avec 0

survient si et seulement si $\rho = \sigma$ et on dit alors qu'ils sont indistinguables.
La distance de trace a la propriété d'être télescopique, c'est-à-dire :

Lemme 2.1. *Pour tout état* ρ_1, ρ_2, σ_1 *et* σ_2*,*

$$\delta(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) \leq \delta(\rho_1, \sigma_1) + \delta(\rho_2, \sigma_2). \tag{2.25}$$

De plus, c'est une fonction monotone sous la trace partielle.

Lemme 2.2. *Pour* $\mathrm{tr}_{\mathcal{B}}(\rho_{\mathcal{AB}}) = \rho_{\mathcal{A}}$ *et* $\mathrm{tr}_{\mathcal{B}}(\sigma_{\mathcal{AB}}) = \sigma_{\mathcal{A}}$*,*

$$\delta(\rho_{\mathcal{A}}, \sigma_{\mathcal{A}}) \leq \delta(\rho_{\mathcal{AB}}, \sigma_{\mathcal{AB}}). \tag{2.26}$$

Finalement, la distance de trace est fortement convexe.

Lemme 2.3. *Pour deux distributions d'états quantiques,* $\{P_{\mathsf{X}_1}(x), \rho^x\}_x$ *et* $\{P_{\mathsf{X}_2}(x), \sigma^x\}_x$*,*

$$\delta\left(\sum_x P_{\mathsf{X}_1}(x)\rho^x, \sum_x P_{\mathsf{X}_2}(x)\sigma^x\right) \leq \sum_x |P_{\mathsf{X}_1}(x) - P_{\mathsf{X}_2}(x)| + \sum_x P_{\mathsf{X}_1}(x)\delta(\rho^x, \sigma^x). \tag{2.27}$$

2.2.9 Résumé

Ce chapitre a premièrement servi à définir ce qu'est un état dans le monde quantique. Un état est soit pur ou mixte s'il est le résultat d'une distribution de probabilité. Par la suite, les concepts de mesure, d'évolution et de purification ont étés introduits. Ceux-ci permettent de décrire comment les systèmes interagissent avec l'environnement. Finalement, nous avons défini une mesure de distance, la distance de trace, qui permet de comparer deux états. Nous avons vu des propriétés de cette fonction qui seront utilisées dans les chapitres suivants.

2.3 Information quantique

Dans cette section, nous présenterons les analogues quantiques de l'entropie de Shannon et de l'information mutuelle. L'entropie quantique et les concepts qui en découlent débutent par le livre sur les fondements de la mécanique quantique par John Von Neumann [23]. Les travaux de Nicolas Cerf et Chris Adami [6], [5] ont permis la généralisation des concepts vus à la section 2.1. Le livre «*Quantum Information Theory*»par Wilde [31] couvre tous les concepts en détail et contient toutes les preuves des résultats qui sont introduits dans cette section.

2.3.1 Entropie de Von Neumann

Soit un état mixte exprimé sous sa forme spectrale $\rho = \sum_x \lambda_x |x\rangle\langle x|$ où les λ_x sont les valeurs propres et $\{|x\rangle\}_x$ est une base orthonormée. Comme nous avons vu dans la section 2.2.4, un état mixte peut-être considéré comme l'état du point de vue d'un observateur externe recevant $|x\rangle$ avec probabilité λ_x. La source produisant cet état contient donc de l'aléa. Une quantité qui représente l'incertitude de l'état quantique est l'entropie de Von Neumann, introduite dans [23].

Définition 2.16 (Entropie de Von Neumann)**.** *L'entropie de Von Neumann de $\rho_{\mathcal{A}}$, notée $S(\rho_{\mathcal{A}})$, est la quantité suivante :*

$$S(\rho_{\mathcal{A}}) = -\operatorname{tr}\left(\rho_{\mathcal{A}} \lg \rho_{\mathcal{A}}\right). \tag{2.28}$$

Cette quantité a des unités de qubits.

L'entropie sous la forme qu'elle prend dans sa définition en (2.28) est, en pratique, difficile à calculer. Par contre, si on exprime ρ sous sa forme spectrale

$$\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|,$$

il est alors facile de calculer $S(\rho)$. Soit I, la source qui produit $|\psi_i\rangle$ avec probabilité λ_i. On a

$$S(\rho) = H(\lambda_i) = H(I). \tag{2.29}$$

Comme décrit dans la section 2.2.4, les valeurs propres peuvent être vues comme une distribution de probabilité sur l'état pur $|\psi_i\rangle$ produit par une source aléatoire I. L'entropie de Von Neumann se réduit donc à l'entropie de Shannon de la variable classique I. Voyons maintenant quelques propriétés utiles de $S(\rho)$. Une conséquence de la forme (2.29) est que, pour tout état pur $|\psi\rangle$, $S(|\psi\rangle\langle\psi|) = 0$. Puisque l'état pur a une valeur propre de $\lambda = 1$,

$$S(|\psi\rangle\langle\psi|) = H(\lambda) = H(1) = 0.$$

L'entropie de Von Neumann est également invariante sous évolution unitaire.

Lemme 2.4. *Soit une transformation unitaire U et un état ρ. Alors,*

$$S(\rho) = S(U\rho U^\dagger). \tag{2.30}$$

Une troisième propriété est la concavité de l'entropie.

Lemme 2.5. *Soit ρ, une matrice densité, alors*

$$S(\rho) \geq \sum_x p_x S(\rho^x) \tag{2.31}$$

pour $\rho = \sum_x p_x \rho^x$.

Nous ferons dans les sections suivantes un raccourci de notation. Pour un état $\rho_{\mathcal{A}}$, la quantité $S(\mathcal{A})_\rho \equiv S(\rho_{\mathcal{A}})$ sert à expliciter l'entropie de ρ sur le registre $\mathcal{A}$. L'indice de $S(\mathcal{A})_\rho$ peut parfois être omis lorsqu'il n'y a aucune ambiguïté sur l'état en question.

2.3.2 Entropie conjointe quantique

L'entropie conjointe de Von Neumann quantifie l'information quantique qui est présente dans un état à multiples registres.

Définition 2.17 (Entropie conjointe quantique)**.** *L'entropie conjointe $S(\mathcal{AB})_\rho$ est l'entropie de Von Neumann sur l'état conjoint des registres $\mathcal{A}$ et $\mathcal{B}$. En d'autres mots*

$$S(\mathcal{AB})_\rho = S(\rho_{\mathcal{AB}}) = -\operatorname{tr}\left(\rho_{\mathcal{AB}} \lg \rho_{\mathcal{AB}}\right)$$

L'entropie marginale $S(\mathcal{A})_\rho$ de $\rho_{\mathcal{AB}}$ se calcule par la trace partielle sur $\mathcal{B}$. Les états purs possèdent une propriété particulière en relation avec l'entropie marginale.

Théorème 2.3. *Les entropies marginales $S(\mathcal{A}_1)_\psi$ et $S(\mathcal{A}_2)_\psi$ d'un état pur $|\psi\rangle_{\mathcal{A}_1\mathcal{A}_2}$ sur les registres $\mathcal{A}_1$ et $\mathcal{A}_2$ sont égales.*

$$S(\mathcal{A}_1)_\psi = S(\mathcal{A}_2)_\psi \tag{2.32}$$

Ce résultat indique que peu importe comment on sépare les registres d'un état pur en deux, les entropies marginales de ceux-ci sont égales. Par exemple, pour un état $|\psi\rangle_{\mathcal{ABC}}$, on a

$$\begin{aligned} S(\mathcal{A}) &= S(\mathcal{BC}) \\ S(\mathcal{B}) &= S(\mathcal{AC}) \\ S(\mathcal{C}) &= S(\mathcal{AB}). \end{aligned}$$

2.3.3 Entropie conditionnelle quantique

Comme dans le cas classique, l'entropie conditionnelle de $\mathcal{A}$ étant donné un registre $\mathcal{B}$ est définie comme suit.

Définition 2.18 (Entropie conditionnelle)**.** *L'entropie conditionnelle $S(\mathcal{A}|\mathcal{B})_\rho$ est l'en-*

tropie conjointe de $(\mathcal{A}, \mathcal{B})$ *moins l'entropie de* $\mathcal{B}$*.*

$$S(\mathcal{A}|\mathcal{B}) = S(\mathcal{A}\mathcal{B}) - S(\mathcal{B}). \tag{2.33}$$

Voyons maintenant des états comportant une partie classique et une quantique.

Définition 2.19 (État classique-quantique)**.** *Un état classique-quantique (C-Q) est un état avec un registre classique* (X) *et un quantique* $(\mathcal{B})$ *conditionné sur la valeur cette première. Tout état C-Q admet une forme*

$$\rho_{X\mathcal{B}} = \sum_{x \in \mathcal{X}} P_{\mathsf{X}}(x) |x\rangle\langle x|_X \otimes \rho^x_{\mathcal{B}}. \tag{2.34}$$

Les états C-Q admettent une forme d'entropie conditionnelle simple.

Lemme 2.6. *L'entropie conditionnelle d'un registre quantique* $\mathcal{B}$ *provenant d'un état C-Q étant donné la variable classique* X *est*

$$S(\mathcal{B}|X) = \sum_x p_x S(\mathcal{B}|X = x) = \sum_x p_x S(\rho^x_{\mathcal{B}}). \tag{2.35}$$

Ce dernier théorème sera utile pour la section suivante dans la discussion sur la borne d'Holevo.

2.3.4 Information mutuelle quantique

En cryptographie, l'information mutuelle est un outil qui permet de quantifier la connaissance qu'un adversaire a à propos d'un secret partagé. Par exemple, si Alice a X et Bob a un état quantique conditionné sur la partie d'Alice. Un tel état a la forme

$$\rho_{X\mathcal{B}} = \sum_x p(x) |x\rangle\langle x|_X \otimes \rho^x_{\mathcal{B}}. \tag{2.36}$$

Nous voulons capturer l'information quantique que Bob a par rapport à x. L'information mutuelle quantique servira à quantifier celle-ci.

Définition 2.20 (Information mutuelle quantique)**.** *L'information mutuelle entre deux registres $\mathcal{A}$ et $\mathcal{B}$ est donnée par la réduction d'entropie sur $\mathcal{A}$ suivant l'obtention de $\mathcal{B}$. En d'autres mots,*

$$S(\mathcal{A};\mathcal{B}) = S(\mathcal{A}) - S(\mathcal{A}|\mathcal{B}). \tag{2.37}$$

Si Alice et Bob partagent l'état en (2.36) alors $S(X;\mathcal{B})$ est le montant de qubit que Bob a à propos de X.

Introduisons un corollaire au théorème (2.6) de la section précédente.

Corollaire 2.2. *L'information mutuelle entre les registres classique et quantique d'un état C-Q $\sum_x p_x |x\rangle\langle x|_X \otimes \rho_{\mathcal{B}}^x$ est*

$$S(X;\mathcal{B}) = S(\mathcal{B}) - \sum_x p_x S(\rho_{\mathcal{B}}^x). \tag{2.38}$$

En effet, $S(X;\mathcal{B}) = S(\mathcal{B}) - S(\mathcal{B}|X)$ et par le théorème (2.6) on obtient directement (2.38). Les états C-Q sont utilisés pour démontrer une limite supérieure sur la quantité d'information classique que nous pouvons extraire d'un état quantique.

Théorème 2.4 (Holevo [14])**.** *Supposons qu'un état quantique ρ_B^x est préparé conditionnellement à la variable classique $X = \{0, 1, \cdots, n\}$ avec la probabilité $\{p_0, \cdots, p_n\}$. Une mesure par un POVM quelconque $\{\Pi_y\}_{y=0}^n$ est appliquée sur le registre $\mathcal{B}$ pour donner le résultat classique Y. Alors,*

$$H(X;Y) \leq S(\rho_{\mathcal{B}}) - \sum_x p_x S(\rho_{\mathcal{B}}^x), \tag{2.39}$$

avec $\rho_{\mathcal{B}} = \sum_x p_x \rho_{\mathcal{B}}^x$. Cette borne est appelée la borne d'Holevo.

De cette borne, nous voyons que le résultat de toute mesure par POVM ne peut révéler plus d'information que l'information mutuelle quantique entre X et $\mathcal{B}$. Ainsi, si Bob

tente d'extraire de l'information classique de son registre $\mathcal{B}$ de l'état en (2.36), il ne peut obtenir plus de $S(X;\mathcal{B})$ bits d'information. La différence entre la borne supérieure et ce qu'il a obtenu par une telle mesure servira de quantité importante dans l'analyse des primitives cryptographiques réalisées quantiquement. Nous l'appellerons la fuite d'information.

2.3.5 Théorèmes fondamentaux de l'information quantique

Avant d'en finir avec la théorie de l'information quantique, nous énoncerons deux théorèmes extrêmement importants pour la suite des travaux. Le premier s'agit de l'inégalité du traitement de l'information quantique. Rappelons les évolutions bruitées de la section 2.2.7. Une évolution bruitée $T^{\mathcal{B}\to\mathcal{B}_1}(\rho)$ prend un état $\rho_{\mathcal{AB}}$ et transmet le résultat d'un processus bruité $\rho_{\mathcal{AB}_1}$, où $\mathcal{B}_1$ n'est pas nécessairement le même espace d'Hilbert que $\mathcal{B}$.

L'information mutuelle entre les registres $\mathcal{A}$ et $\mathcal{B}$ peut-elle grandir suite à l'application d'une telle évolution ? Il s'avère que l'information peut augmenter si une telle évolution est appliquée à un état. Le théorème sur le traitement de l'information quantique est le suivant.

Théorème 2.5. *Soit les états $\rho_{\mathcal{AB}}$, $\phi_{\mathcal{AB}_1} = T_1^{\mathcal{B}\to\mathcal{B}_1}(\rho_{\mathcal{AB}})$ et $\sigma_{\mathcal{AB}_2} = T_2^{\mathcal{B}_1\to\mathcal{B}_2}(\phi_{\mathcal{AB}_1})$. Alors l'inégalité suivante est respectée pour toute évolution $T_1^{\mathcal{B}\to\mathcal{B}_1}(\cdot)$ et $T_2^{\mathcal{B}_1\to\mathcal{B}_2}(\cdot)$:*

$$S(\mathcal{A};\mathcal{B})_\rho \geq S(\mathcal{A};\mathcal{B}_1)_\phi \geq S(\mathcal{A};\mathcal{B}_2)_\sigma \tag{2.40}$$

Ce que ce théorème démontre, c'est que les évolutions bruitées ne peuvent pas augmenter l'information mutuelle entre deux registres d'un même état. Un corollaire important est le suivant.

Corollaire 2.3. *Soient $\rho_{\mathcal{AB}_1\mathcal{B}_2}$ et $\sigma_{\mathcal{AB}_1} = \mathrm{tr}_{\mathcal{B}_2}(\rho_{\mathcal{AB}_1\mathcal{B}_2})$, l'état résultant de la trace partielle sur $\mathcal{B}_2$ de ρ. Alors,*

$$S(\mathcal{A};\mathcal{B}_1\mathcal{B}_2) \geq S(\mathcal{A};\mathcal{B}_1) \tag{2.41}$$

l'information que $\mathcal{B}_1\mathcal{B}_2$ contient à propos de $\mathcal{A}$ est plus grande ou égale à l'information que seulement $\mathcal{B}_1$ contient.

La perte d'un registre quantique a donc effet de réduire la quantité d'information. Le résultat qui suit permet de quantifier la différence entre des quantités entropiques si la distance de trace est connue. Ce théorème apporte donc une notion de continuité à l'entropie de Von Neumann.

Théorème 2.6. *Pour tout états $\rho_{\mathcal{AB}}$ et $\sigma_{\mathcal{AB}}$ avec $\delta(\rho_{\mathcal{AB}}, \sigma_{\mathcal{AB}}) \leq \epsilon$,*

$$|S(\mathcal{A};\mathcal{B})_\rho - S(\mathcal{A};\mathcal{B})_\sigma| \leq 6\epsilon \lg d_{\mathcal{A}} + 4H(\epsilon) \tag{2.42}$$

où $H(\epsilon)$ est l'entropie de Shannon de la distribution $\{\epsilon, 1-\epsilon\}$ et $d_{\mathcal{A}}$ la dimension du registre $\mathcal{A}$.

Cette inégalité est appelée l'inégalité de Alicki-Fannes pour l'information mutuelle quantique [1].

2.3.6 Résumé

Dans cette section, nous avons introduit les analogues quantiques aux outils en théorie de l'information classique. De plus, nous avons vu la borne d'Holevo qui dicte combien d'information classique on peut extraire d'un état quantique. Finalement, deux théorèmes fondamentaux ont été présentés : le théorème sur le traitement de l'information quantique et l'inégalité d'Alick-Fannes.

CHAPITRE 3

RÉALISATIONS DE PRIMITIVES ET MONOTONES

Ce chapitre aura comme but de présenter formellement les résultats connus introduits brièvement au chapitre 1. Les résultats présentés proviennent de Wolf et Wullschleger [32], [33] pour la version classique et par Salvail et al. [26] pour la version quantique.

3.1 Monotones classiques

Rappelons premièrement ce qu'est une primitive cryptographique dans le modèle HMC. Une primitive est une tâche qui représente le calcul d'une fonction $f : \mathcal{A} \times \mathcal{B} \to \mathcal{X}' \times \mathcal{Y}'$ à deux parties. Cette fonction a des entrées a, b et des sorties x', y' chez Alice et Bob respectivement. Dans ce cas-ci, nous prenons les entrées au hasard, $a \in_R \mathcal{A}$ et $b \in_R \mathcal{B}$, et les donnons en sortie aux participants. Alice reçoit alors une paire $x = (a, x')$ et Bob reçoit $y = (b, y')$. La primitive produit deux variables aléatoires : $X = (A, X')$ et $Y = (B, Y')$. On définit alors une primitive par sa distribution de probabilité

$$P_{\mathsf{X},\mathsf{Y}}(x, y) \coloneqq Pr(X = (a, x'), Y = (b, y')) \tag{3.1}$$

où $a \in_R \mathcal{A}$ et $b \in_R \mathcal{B}$. Dans ce cas-ci, a est pris avec probabilité $1/|\mathcal{A}|$ et b avec probabilité $1/|\mathcal{B}|$. On dit que A, B et C, trois distributions, forment une chaîne de Markov si elles respectent la définition suivante.

Définition 3.1 (Chaîne de Markov [8])**.** *$A \leftrightarrow B \leftrightarrow C$ est une chaîne de Markov si A et C sont indépendants étant donné B. En d'autres mots, les conditions équivalentes*

suivantes sont respectées :

$$\begin{aligned} P(AC|B) &= P(A|B)P(C|B), \\ P(A|BC) &= P(A|B), \\ P(C|AB) &= P(C|B). \end{aligned}$$

Les chaînes de Markov seront utiles pour mettre en relation les quantités définies ci-bas.

Définition 3.2 (Partie dépendante [32])**.** *La partie dépendante de X sur Y, notée $X \searrow Y$, est la partie de X qui est corrélée avec Y. Plus formellement, soit $f(x) = P_{\mathsf{Y}|\mathsf{X}=x}$,*

$$X \searrow Y \equiv f(X). \tag{3.2}$$

La partie dépendante, aussi appelée *statistique suffisante*, est la variable aléatoire qui est obtenue par l'effondrement de toutes les valeurs x_1 et x_2 telles que $f(x_1) = f(x_2)$. Ceci permet de décrire la dépendance de X sur Y, car s'ils sont indépendants,

$$f(X) = P_{\mathsf{Y}|\mathsf{X}} = P_{\mathsf{Y}}.$$

Définition 3.3 (Composantes connexes [32])**.** *Soit les variables X et Y et leur alphabet respectif $\mathcal{X}$ et $\mathcal{Y}$ distribué selon $P_{\mathsf{X},\mathsf{Y}}$. Le graphe biparti G est construit avec les sommets $\mathcal{X} \cup \mathcal{Y}$ tels que tous sommets $x \in \mathcal{X}$ et $y \in \mathcal{Y}$ sont connectés par une arête si et seulement si $P_{\mathsf{X},\mathsf{Y}}(x, y) > 0$. Nous définissons $f_X(x)$ comme étant la fonction qui prend un sommet $x \in \mathcal{X}$ et qui produit la composante connexe du graphe G auquel x appartient. $f_Y(y)$ est défini de façon similaire. La composante connexe de $P_{\mathsf{X},\mathsf{Y}}$, notée $X \wedge Y$, est*

$$X \wedge Y = f_X(X) = f_Y(Y). \tag{3.3}$$

Cette variable aléatoire qualifie donc l'ensemble des sous-graphes de G qui décrivent les sous-distributions de $P_{\mathsf{X},\mathsf{Y}}$. Cette fonction est symétrique puisque les composantes

connexes de G sont accessible à partir de $\mathcal{X}$ et de $\mathcal{Y}$.
Wolf et Wullschleger [32], [33] démontrent que la partie dépendante et les composantes connexes peuvent être utilisées pour définir des monotones sur les primitives cryptographiques. Une monotone est une quantité qui ne peut croitre par du calcul et de la communication sans bruit.

Théorème 3.1 (Wolf et Wullschleger [33])**.** *Soit une primitive $P_{\mathsf{X},\mathsf{Y}}$ produisant en sortie X et Y selon la distribution de probabilité $P_{\mathsf{X},\mathsf{Y}}(x,y)$. Notons X' et Y' les variables suite à un second protocole utilisant de la communication et du calcul sans bruit. Alors, les inégalités suivantes sont respectées :*

$$\begin{aligned} H(X' \searrow Y'|Y') &\leq H(X \searrow Y|Y), \\ H(Y' \searrow X'|X') &\leq H(Y \searrow X|X), \\ I(X';Y'|X' \wedge Y') &\leq I(X;Y|X \wedge Y). \end{aligned}$$

Les trois quantités entropiques ci-haut permettent de hiérarchiser les primitives de la façon suivante : Une primitive $P_{\mathsf{X},\mathsf{Y}}$ ne peut pas être réalisée à l'aide d'un seul appel à une seconde primitive $P_{X',Y'}$ si l'une des inégalités ci-haut est fausse. Par contradiction, imaginons que c'est possible. Alors, la ou les quantités qui brisent les inégalités ci-haut contredisent le théorème, car il est possible de faire croître leur valeur à l'aide de communication et de calcul sans bruit. Terminons par définir le concept de primitive triviale.

Définition 3.4 (Primitive triviale)**.** *Une primitive $P_{\mathsf{X},\mathsf{Y}}$ est triviale si elle satisfait*

$$H(Y \searrow X|X) = 0$$

ou de façon équivalente,

$$H(X \searrow Y|Y) = 0.$$

Dans le cas contraire, on dit que la primitive est non triviale.

Intuitivement, cette définition dit qu'une primitive est triviale si elle est réalisable à partir de rien. Puisque sa monotone est minimale, elle ne peut pas être utilisée pour construire une primitive non triviale. Dans cette optique, elle ne possède pas de puissance de calcul. Les monotones ne quantifient pas la complexité d'une primitive. Par exemple, il existe des travaux par Mochon [21] et Chailloux et Kerenidis [7] portant sur la primitive de pièce aléatoire qui énonce des protocoles particulièrement non triviaux en complexité alors que la primitive, selon notre définition, est triviale.

3.2 Monotone quantique

La section précédente offre un contexte intéressant à la question de hiérarchie des primitives cryptographiques à deux parties classiques. Nous avons vu qu'il existe des quantités monotones définies sur les sorties d'un protocole classique. Le même scénario s'applique pour ces mêmes primitives, lorsque réalisées quantiquement.

3.2.1 États stricts-corrects

Nous introduirons dans cette section les travaux de Salvail, Schaffner et Sotàkovà [26]. Ceux-ci démontrent qu'une quantité monotone existe pour les états stricts-corrects. Ces travaux servent de point de départ pour les résultats présentés dans le cadre de ce mémoire. Mentionnons également que les réalisations quantiques sont faites dans le cadre du modèle QHMC introduit au chapitre 1.

Une primitive classique réalisée quantiquement est un protocole qui, avec du calcul et de la communication quantique, produit un état quantique en sortie. Alice et Bob doivent mesurer leurs registres pour obtenir les sorties classiques X et Y.

Les monotones quantiques sont reliées à l'information quantique que les participants possèdent. Dans cette optique, nous permettons aux participants de purifier leurs états et de conserver les registres auxiliaires ainsi créés. L'information mutuelle entre les sorties

ne peut qu'augmenter s'ils conservent les systèmes de purification. Nous assumons que tout état produit par la réalisation quantique d'une primitive est pur.

Nous appliquons aussi la restriction suivante : pour obtenir leur sortie, Alice et Bob doivent mesurer leur registre dans la base calculatoire. S'ils mesuraient dans une base différente, ils pourraient appliquer la transformation unitaire appropriée avant de mesurer dans la base $\{|0\rangle, |1\rangle\}$ pour produire la même distribution. Le résultat de la mesure est la sortie classique du modèle HMC, soit X et Y selon la distribution $P_{\mathsf{X},\mathsf{Y}}$. Utilisant le modèle QHMC, les états quantiques produits par Alice et Bob réalisant la primitive cryptographique $P_{\mathsf{X},\mathsf{Y}}$ sont tous de la forme :

$$|\psi\rangle_{\mathcal{A}\mathcal{B}\mathcal{A}'\mathcal{B}'} = \sum_{x,y} \sqrt{P_{\mathsf{X},\mathsf{Y}}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}} \otimes |\phi_{x,y}\rangle_{\mathcal{A}'\mathcal{B}'}. \tag{3.4}$$

Où $\theta(x,y)$ est une fonction qui associe chaque paire (x,y) à un angle $\theta \in [0...2\pi)$. La probabilité qu'Alice et Bob mesurent (x,y) en utilisant la base calculatoire est donc

$$\left(\sqrt{P_{\mathsf{X},\mathsf{Y}}(x,y)} e^{i\theta(x,y)} \right)^2 = P_{\mathsf{X},\mathsf{Y}}(x,y),$$

telle que requise par le modèle QHMC. Nous appelons les états de la forme (3.4) une enveloppe pour la distribution $P_{\mathsf{X},\mathsf{Y}}$.

Une enveloppe, en général, peut, suite à la mesure des registres $\mathcal{A}$ et $\mathcal{B}$, contenir de l'information résiduelle dans les registres auxiliaires $\mathcal{A}'$ et $\mathcal{B}'$. L'état $|\phi_{x,y}\rangle$ peut être utilisé pour récupérer de l'information additionnelle par un participant curieux. Un protocole π qui produit une enveloppe dont les registres $\mathcal{A}'\mathcal{B}'$ ne contiennent aucune information dans le scénario honnête est appelé *strict-correct*.

Définition 3.5 (Strict-correct)**.** *Un protocole π pour la primitive $P_{\mathsf{X},\mathsf{Y}}$ est strict-correct si la mesure de $\mathcal{A}$ et $\mathcal{B}$ dans la base calculatoire produit (x,y) avec probabilité $P_{\mathsf{X},\mathsf{Y}}(x,y)$*

et l'état suite à la mesure respecte

$$S(X;Y\mathcal{B}') = S(X\mathcal{A}';Y) = I(X;Y). \tag{3.5}$$

L'enveloppe produisant cette égalité est aussi appelée stricte-correcte.

L'extension quantique des chaînes de Markov est présentée par Damgård et al. [10] et par Fehr et Schaffner [13]. Un état C-C-Q (classique-classique-quantique)

$$\sum_{x,y} P(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_{\mathcal{R}}^{x,y}$$

forme la chaîne de Markov $X \leftrightarrow Y \leftrightarrow \mathcal{R}$ si le registre $\mathcal{R}$ ne dépend pas de la variable classique x. En d'autres mots, $\rho_{\mathcal{R}}^{x,y} \equiv \rho_{\mathcal{R}}^{y}$.

Lemme 3.1. *Les conditions suivantes sont équivalentes pour un état C-C-Q :*

1. $X \leftrightarrow Y \leftrightarrow \mathcal{R}$
2. $S(X|Y\mathcal{R}) = H(X|Y)$
3. $S(\mathcal{R}|XY) = S(\mathcal{R}|Y)$
4. $S(X;Y\mathcal{R}) = I(X;Y)$

Un état strict-correct, par la condition 4, est donc une enveloppe qui suite à la mesure des variables classiques X et Y, a la propriété d'être la chaîne de Markov suivante : $\mathcal{A}' \leftrightarrow X \leftrightarrow Y \leftrightarrow \mathcal{B}'$.
On appelle une enveloppe régulière tout état dont $\mathcal{A}'$ et $\mathcal{B}'$ sont vides. Ces états sont trivialement stricts-corrects et seront importants dans l'analyse de la fuite d'information.

Définition 3.6 (Enveloppe régulière)**.** *L'ensemble des enveloppes régulières pour une distribution conjointe $P_{\mathsf{X},\mathsf{Y}}$, où $X \in \{0,1\}^n$ et $Y \in \{0,1\}^m$, est défini par*

$$\epsilon\left(P_{\mathsf{X},\mathsf{Y}}\right) \equiv \left\{ |\psi\rangle \in \mathcal{H}_{\mathcal{AB}} : |\psi\rangle = \sum_{x\in\{0,1\}^n, y\in\{0,1\}^m} \sqrt{P_{\mathsf{X},\mathsf{Y}}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}}, \theta \in \Theta_{n,m} \right\}, \tag{3.6}$$

où $\Theta_{n,m} \coloneqq \{\theta : \{0,1\}^n \times \{0,1\}^m \to [0 \cdots 2\pi)\}$ *est l'ensemble des fonctions qui prennent des chaînes de bits de longueur* $n+m$ *et qui produisent un nombre réel entre* 0 *et* 2π. *L'état dont* $\theta(x,y) = 0$ *pour tout* (x,y) *est appelée l'enveloppe canonique.*

Le concept de primitive triviale pour une réalisation classique a été défini par Wolf et Wullschleger dans [32]. L'extension quantique est la suivante :

Définition 3.7 (Enveloppe triviale)**.** *Une enveloppe régulière* $|\psi\rangle \in \epsilon\left(P_{\mathsf{X},\mathsf{Y}}\right)$ *est appelée triviale si soit*

$$S(X \searrow Y|\mathcal{B}) = 0,$$

ou

$$S(Y \searrow X|\mathcal{A}) = 0.$$

Autrement, $|\psi\rangle$ *est dite non-triviale.*

Lemme 3.2. *Si* $P_{\mathsf{X},\mathsf{Y}}$ *est une primitive non triviale alors son enveloppe canonique* $|\psi_0\rangle \in \epsilon\left(P_{\mathsf{X},\mathsf{Y}}\right)$ *est également non-triviale.*

Un participant dans le modèle QHMC obtiendra toujours au moins $I(X;Y)$ bits d'information sur le résultat de son partenaire. Une enveloppe qui possède des registres de purification contient autant sinon plus d'information quantique. Ce fait découle du théorème d'Holevo (2.4). La fuite d'information capture l'information qui serait accessible à un participant malhonnête qui ne mesurerait pas sa partie principale dans la base calculatoire.

Définition 3.8 (Fuite d'information d'une enveloppe)**.** *Soit une enveloppe* $|\psi\rangle \in \mathcal{H}_{\mathcal{A}\mathcal{B}\mathcal{A}'\mathcal{B}'}$ *de* $P_{\mathsf{X},\mathsf{Y}}$. *La fuite d'information de* $|\psi\rangle$ *est*

$$\Delta_\psi(P_{\mathsf{X},\mathsf{Y}}) \coloneqq \max\{S(X;\mathcal{B}\mathcal{B}') - I(X;Y), S(\mathcal{A}\mathcal{A}';Y) - I(X;Y)\}. \tag{3.7}$$

On dit que $|\psi\rangle$ *fuit* δ *si* $\Delta_\psi(P_{\mathsf{X},\mathsf{Y}}) \geq \delta$.

Pour des états stricts-corrects, il s'avère que les deux quantités dans (3.7) sont égales.

Lemme 3.3. *La fuite d'information d'une enveloppe* $|\psi\rangle \in \mathcal{H}_{\mathcal{AB}\mathcal{A}'\mathcal{B}'}$ *de* $P_{\mathsf{X},\mathsf{Y}}$ *qui est stricte-correcte est*

$$\Delta_{\psi}(P_{\mathsf{X},\mathsf{Y}}) = S(X;\mathcal{B}\mathcal{B}') - I(X;Y) = S(\mathcal{A}\mathcal{A}';Y) - I(X;Y).$$

Si Alice et Bob roulent un protocole qui produit une purification stricte-correcte, ils observeront une fuite d'information identique. Ceci ne s'appliquera pas quand nous considérerons des états qui ne satisfont pas la condition de la définition 3.5. Un autre lemme montre que pour tout état strict-correct, sa fuite est bornée inférieurement par la fuite d'une enveloppe régulière de la même distribution conjointe $P_{\mathsf{X},\mathsf{Y}}$.

Lemme 3.4. *Pour toute enveloppe* $|\psi\rangle$ *d'une primitive* $P_{\mathsf{X},\mathsf{Y}}$ *il existe* $|\psi^*\rangle \in \epsilon\,(P_{\mathsf{X},\mathsf{Y}})$ *telle que* $\Delta_{\psi}(P_{\mathsf{X},\mathsf{Y}}) \geq \Delta_{\psi^*}(P_{\mathsf{X},\mathsf{Y}})$.

La fuite d'information, jusqu'ici définie pour une purification particulière, atteint un minimum parmi les enveloppes régulières. Puisque nous désirons avoir une mesure monotone qui, comme dans le cas classique, permet de classifier les primitives selon leur puissance de calcul, définissons alors la fuite d'information pour une primitive.

Définition 3.9 (Fuite d'information d'une primitive)**.** *La fuite d'information d'une primitive* $P_{\mathsf{X},\mathsf{Y}}$ *est le minimum atteint par des enveloppes régulières, soit*

$$\Delta_{P_{\mathsf{X},\mathsf{Y}}} \coloneqq \min_{|\psi\rangle} \Delta_{\psi}(P_{\mathsf{X},\mathsf{Y}}) \tag{3.8}$$

où les $|\psi\rangle$ *sont stricts-corrects.*

L'analogue quantique au théorème 3.1 énonce une forme de réductibilité et met en relation la fuite d'information des primitives qui sont réalisables selon cette notion.

Théorème 3.2 (Salvail et al. [26])**.** *Si deux primitives $P_{\mathsf{X},\mathsf{Y}}$ et $P_{\tilde{\mathsf{X}}_1\tilde{\mathsf{X}}_2,\tilde{\mathsf{Y}}_1\tilde{\mathsf{Y}}_2}$ respectent la condition suivante*

$$\sum_{\substack{x,y:\\ P_{\tilde{\mathsf{X}}_2,\tilde{\mathsf{Y}}_2|\tilde{\mathsf{X}}_1=\mathsf{X},\tilde{\mathsf{Y}}_1=\mathsf{Y}}\simeq P_{\mathsf{X},\mathsf{Y}}}} P_{\tilde{\mathsf{X}}_1,\tilde{\mathsf{Y}}_1}(x,y) \geq 1-\delta,$$

où $\simeq$ signifie que les distributions sont identiques à un réétiquetage de leur alphabet près, alors

$$\Delta_{P_{\tilde{\mathsf{X}}_1\tilde{\mathsf{X}}_2,\tilde{\mathsf{Y}}_1\tilde{\mathsf{Y}}_2}} \geq (1-\delta)\Delta_{P_{\mathsf{X},\mathsf{Y}}}. \tag{3.9}$$

Il existe donc une notion de réduction selon laquelle la fuite d'information agit comme une monotone pour les purifications strictes-correctes de primitives classiques.

3.3 Résumé

Les primitives cryptographiques sont des tâches produisant une sortie chez Alice et une chez Bob. Si elles sont réalisées classiquement, Wolf et Wullschleger [32], [33] ont démontré qu'il existe des quantités qui ne peuvent augmenter suite au protocole. Celles-ci permettent de hiérarchiser les primitives par leur puissance de calcul. Quantiquement, Salvail et al. [26] ont démontré qu'une quantité analogue existe si on se limite aux états stricts-corrects. Dans les chapitres suivants, une étude des états corrects servira à explorer comment la fuite d'information agit lorsque nous relaxons la condition sur la fuite dans le cas honnête.

CHAPITRE 4

FUITE D'INFORMATION DES ÉTATS CORRECTS

Ce chapitre explore la relation entre la fuite d'information des enveloppes strictes-correctes et des états corrects. En premier lieu, nous introduisons le concept d'ϵ-enveloppe. Cette mesure de dépendance sur x et y des registres auxiliaires permettra d'établir la continuité de la fuite d'information. Finalement, nous démontrons que pour certains états corrects, il existe un état strict-correct qui ne fuit pas plus d'information que ceux-ci. Ce dernier résultat sert à démontrer que les résultats de Salvail et al. [26] s'appliquent au moins à un sous-ensemble des états corrects en plus des états stricts-corrects.

4.1 État correct

Les états corrects sont des états qui ont la forme générale

$$|\psi\rangle_{\mathcal{AB}\mathcal{A}'\mathcal{B}'} = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}} \otimes |\phi_{x,y}\rangle_{\mathcal{A}'\mathcal{B}'}. \tag{4.1}$$

Ce sont des enveloppes qui, par la mesure de $\mathcal{A}$ et $\mathcal{B}$ dans la base calculatoire, produisent X et Y selon la distribution de probabilité $P_{X,Y}$. La différence avec les états stricts-corrects est la relaxation de la condition que la fuite est nulle si Alice et Bob sont honnêtes. En d'autres mots, les états corrects permettent

$$S(X;Y\mathcal{B}') > I(X;Y)$$

et

$$S(X\mathcal{A}';Y) > I(X;Y).$$

La relaxation de la condition sur l'information résiduelle dans $\mathcal{A}'$ et $\mathcal{B}'$ n'assure plus la symétrie du lemme 3.3. Ainsi, nous dirons que la fuite d'Alice est $\Delta^A_\psi(P_{X,Y}) =$

$S(\mathcal{A}\mathcal{A}';Y) - I(X;Y)$ et la fuite de Bob est $\Delta_\psi^B(P_{X,Y}) = S(X;\mathcal{B}\mathcal{B}') - I(X;Y)$. La fuite de l'état $|\psi\rangle$ est

$$\Delta_\psi(P_{X,Y}) = \max\left\{\Delta_\psi^A(P_{X,Y}), \Delta_\psi^B(P_{X,Y})\right\}.$$

Si $S(\mathcal{A}\mathcal{A}';Y) = I(X;Y)$, alors l'état est strict-correct pour Alice. Nous utiliserons le même langage pour Bob.

4.2 ϵ-enveloppes

Nous sommes intéressés à la dépendance sur x et y de $|\phi_{x,y}\rangle_{\mathcal{A}'\mathcal{B}'}$ à l'équation (4.1). Pour ce faire, prenons le point de vue de Bob d'abord et quantifions la corrélation de son registre auxiliaire avec x. Notons l'état dans les registres $\mathcal{B}\mathcal{B}'$ lorsque x est fixé par

$$\rho_{\mathcal{B}\mathcal{B}'}^x = \mathrm{tr}_{\mathcal{A}\mathcal{A}'}\left((|x\rangle\langle x|_{\mathcal{A}} \otimes \mathbb{1}_{\mathcal{A}'\mathcal{B}\mathcal{B}'})|\psi\rangle\langle\psi|\right). \tag{4.2}$$

Pour quantifier la dépendance de $\rho_{\mathcal{B}\mathcal{B}'}^x$, nous utiliserons un état voisin de $|\psi\rangle$ qui a la forme

$$\left|\tilde{\psi}\right\rangle_{\mathcal{A}\mathcal{B}\mathcal{A}'\mathcal{B}'} = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}} \otimes |\varphi_y\rangle_{\mathcal{A}'\mathcal{B}'} \tag{4.3}$$

comme point de référence. De la même façon qu'en (4.2), on a que

$$\sigma_{\mathcal{B}\mathcal{B}'}^x = \mathrm{tr}_{\mathcal{A}\mathcal{A}'}\left((|x\rangle\langle x|_{\mathcal{A}} \otimes \mathbb{1}_{\mathcal{A}'\mathcal{B}\mathcal{B}'})\left|\tilde{\psi}\right\rangle\left\langle\tilde{\psi}\right|\right). \tag{4.4}$$

Définition 4.1 (Avantage ϵ_B)**.** *Un état $|\psi\rangle$ a un avantage ϵ_B pour Bob où*

$$\epsilon_B = \min_{|\tilde{\psi}\rangle}\left\{\sum_x P_X(x)\delta(\rho_{\mathcal{B}\mathcal{B}'}^x, \sigma_{\mathcal{B}\mathcal{B}'}^x)\right\}. \tag{4.5}$$

Le minimum est pris sur tous les états $|\tilde{\psi}\rangle$ de la forme (4.3) associés à $\sigma_{\mathcal{B}\mathcal{B}'}^x$ défini en (4.4).

Nous définissons d'une façon analogue l'avantage ϵ_A pour le point de vue d'Alice. Pour la dépendance sur y, prenons

$$\rho^y_{\mathcal{A}\mathcal{A}'} = \mathrm{tr}_{\mathcal{B}\mathcal{B}'}\left((|y\rangle\langle y|_{\mathcal{B}} \otimes \mathbb{1}_{\mathcal{A}\mathcal{A}'\mathcal{B}'})|\psi\rangle\langle\psi|\right).$$

Le point de référence sera des états ayant la forme

$$|\bar{\psi}\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}} \otimes |\varphi_x\rangle_{\mathcal{A}'\mathcal{B}'}$$

et la matrice densité sur $\mathcal{A}\mathcal{A}'$ lorsque y est fixé est

$$\sigma^y_{\mathcal{A}\mathcal{A}'} = \mathrm{tr}_{\mathcal{B}\mathcal{B}'}\left((|y\rangle\langle y|_{\mathcal{B}} \otimes \mathbb{1}_{\mathcal{A}\mathcal{A}'\mathcal{B}'})|\bar{\psi}\rangle\langle\bar{\psi}|\right).$$

Ainsi, $|\psi\rangle$ a un avantage ϵ_A pour Alice où

$$\epsilon_A = \min_{|\bar{\psi}\rangle} \left\{ \sum_y P_Y(y) \delta(\rho^y_{\mathcal{A}\mathcal{A}'}, \sigma^y_{\mathcal{A}\mathcal{A}'}) \right\}. \tag{4.6}$$

Définition 4.2 (ϵ-enveloppe)**.** *Soit une enveloppe $|\psi\rangle$ ayant un avantage ϵ_A pour Alice et ϵ_B pour Bob. $|\psi\rangle$ est alors une ϵ-enveloppe pour*

$$\epsilon = \max\{\epsilon_A, \epsilon_B\}.$$

4.3 La continuité de la fuite d'information

Nous nous intéressons à savoir si, pour tout état correct, il existe une enveloppe stricte-correcte dont la fuite d'information est similaire. Notre contribution est le théorème suivant qui établit son existence et borne supérieurement leur différence en valeur absolue.

Théorème 4.1. *Pour toute enveloppe $|\psi\rangle$ avec ϵ_B pour Bob et ϵ_A pour Alice, il existe un*

état $|\phi\rangle$ strict-correct pour Bob tel que

$$\left|\Delta_{\psi}^{B}(P_{X,Y}) - \Delta_{\phi}^{B}(P_{X,Y})\right| \leq 6\epsilon_B|X| + 4H_2(\epsilon_B). \tag{4.7}$$

Il existe aussi un état strict-correct pour Alice, $|\tilde{\phi}\rangle$ tel que

$$\left|\Delta_{\psi}^{A}(P_{X,Y}) - \Delta_{\tilde{\phi}}^{A}(P_{X,Y})\right| \leq 6\epsilon_A|Y| + 4H_2(\epsilon_A). \tag{4.8}$$

Démonstration. Commençons par établir l'existence de $|\phi\rangle$. Ensuite, nous quantifierons la distance de trace entre les matrices densités réduites de celui-ci et de $|\psi\rangle$ sur les registres $X\mathcal{B}\mathcal{B}'$. Ceci permettra d'appliquer le théorème d'Alicki-Fannes pour l'information mutuelle quantique (2.6) et de conclure avec le résultat de l'équation (4.8).
Puisque $|\psi\rangle$ est une ϵ_B-enveloppe pour Bob, prenons $|\phi\rangle$ comme l'état qui minimise la quantité de l'équation (4.5). Ainsi, nous avons que

$$\epsilon_B = \sum_x P_X(x)\delta(\rho_{\mathcal{B}\mathcal{B}'}^x, \sigma_{\mathcal{B}\mathcal{B}'}^x)$$

où les arguments de la distance de trace sont définis en (4.2) et en (4.4). En utilisant les propriétés de la distance de trace, nous arrivons à

$$\begin{aligned}
\epsilon_B &= \sum_x P_X(x)\delta(\rho_{\mathcal{B}\mathcal{B}'}^x, \sigma_{\mathcal{B}\mathcal{B}'}^x) \\
&\geq \sum_x P_X(x)\delta(|x\rangle\langle x|_X \otimes \rho_{\mathcal{B}\mathcal{B}'}^x, |x\rangle\langle x|_X \otimes \sigma_{\mathcal{B}\mathcal{B}'}^x) \\
&\geq \delta\left(\sum_x P_X(x)|x\rangle\langle x|_X \otimes \rho_{\mathcal{B}\mathcal{B}'}^x, \sum_x P_X(x)|x\rangle\langle x|_X \otimes \sigma_{\mathcal{B}\mathcal{B}'}^x\right) \\
&\geq \delta(\rho_{X\mathcal{B}\mathcal{B}'}, \sigma_{X\mathcal{B}\mathcal{B}'}).
\end{aligned}$$

La première inégalité provient du fait que $\delta(|x\rangle\langle x|, |x\rangle\langle x|) = 0$ et de la propriété télescopique de la distance de trace (2.1). La deuxième inégalité provient de la forte convexité établie en (2.3). Finalement, la dernière ligne est due au fait que $\rho_{X\mathcal{B}\mathcal{B}'}$ et $\sigma_{X\mathcal{B}\mathcal{B}'}$ sont les

matrices densités sur les registres $X\mathcal{B}\mathcal{B}'$ suite à la mesure de X.
Nous avons que $\delta(\rho_{X\mathcal{B}\mathcal{B}'}, \sigma_{X\mathcal{B}\mathcal{B}'}) \leq \epsilon_B$. Ceci permet d'appliquer l'inégalité d'Alicki-Fannes pour l'information mutuelle quantique (2.6) et d'obtenir

$$|S(X;\mathcal{B}\mathcal{B}')_\psi - S(X;\mathcal{B}\mathcal{B}')_\phi| \leq 6\epsilon_B \lg d_X + 4H(\epsilon_B).$$

Puisque $\lg d_X = |X|$, la taille de X, et que $\Delta^B_\psi(P_{X,Y}) = S(X;\mathcal{B}\mathcal{B}')_\psi - I(X;Y)$, nous pouvons conclure que

$$\begin{aligned} |S(X;\mathcal{B}\mathcal{B}')_\psi - I(X;Y) - S(X;\mathcal{B}\mathcal{B}')_\phi + I(X;Y)| &\leq 6\epsilon_B|X| + 4H_2(\epsilon_B) \\ \left|\Delta^B_\psi(P_{X,Y}) - \Delta^B_\phi(P_{X,Y})\right| &\leq 6\epsilon_B|X| + 4H_2(\epsilon_B). \end{aligned}$$

□

4.4 État décorrélé

Nous verrons dans cette section la fuite des états décorrélés, un cas spécial d'états stricts-corrects. L'état $|\phi_{x,y}\rangle_{\mathcal{A}'\mathcal{B}'}$, de l'équation (4.1), a la forme

$$|\phi_{x,y}\rangle_{\mathcal{A}'\mathcal{B}'} = \sum_k \lambda_k^{x,y} |e_k^{x,y}\rangle_{\mathcal{A}'} |f_k^{x,y}\rangle_{\mathcal{B}'} \tag{4.9}$$

par la décomposition de Schmidt (2.2). La condition entropique pour les enveloppes strictes-correctes (3.5) implique qu'aucune information résiduelle, une fois que X et Y sont mesurés, n'est contenue dans $\mathcal{A}'$ et $\mathcal{B}'$. Ainsi, pour tout (x, y), $\rho^{x,y}_{\mathcal{B}'} = \rho^{x',y}_{\mathcal{B}'}$. Ceci implique que les valeurs propres de l'équation (4.9) doivent être indépendantes de x. Par un argument analogue, elles doivent également être indépendantes de y. On a donc que $\lambda_k^{x,y} = \lambda_k$. La forme complète des états stricts-corrects devient alors

$$|\psi\rangle_{\mathcal{A}\mathcal{B}\mathcal{A}'\mathcal{B}'} = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}} \otimes \sum_k \sqrt{\lambda_k} e^{i\theta(x,y,k)} |e_k^{x,y}\rangle_{\mathcal{A}'} |f_k^{x,y}\rangle_{\mathcal{B}'}. \tag{4.10}$$

La fonction de phase θ peut, dans la purification de $\rho_{\mathcal{B}'}^{x,y}$, prendre une dépendance sur k. Un état décorrélé est défini à l'aide de l'équation (4.10) ci-haut.

Définition 4.3 (État décorrélé)**.** *Un état décorrélé $|\psi\rangle$ est un état strict-correct (4.10) avec la condition additionnelle que*

$$e^{i\theta(x,y,k)} = e^{i\theta(x,y)}e^{i\theta(k)} \tag{4.11}$$

et

$$\begin{aligned} |e_k^{x,y}\rangle_{\mathcal{A}'} &= |e_k^x\rangle_{\mathcal{A}'}, \\ |f_k^{x,y}\rangle_{\mathcal{B}'} &= |f_k^y\rangle_{\mathcal{B}'}. \end{aligned} \tag{4.12}$$

Le lemme suivant démontre que les registres $\mathcal{A}'$ et $\mathcal{B}'$ ne participent pas dans la fuite d'information des participants respectifs.

Lemme 4.1. *La fuite d'information de tout état décorrélé $|\psi\rangle$ est*

$$\Delta_\psi(P_{X,Y}) = S(X;\mathcal{B}) - I(X;Y) = S(\mathcal{A};Y) - I(X;Y). \tag{4.13}$$

Démonstration. Puisque $|\psi\rangle$ est un cas spécial d'état strict-correct, le lemme 3.3 s'applique et la fuite du côté d'Alice et de Bob est égale. Il ne suffit qu'à démontrer que $S(X;\mathcal{B}\mathcal{B}') = S(X;\mathcal{B})$ et $S(\mathcal{A}\mathcal{A}';Y) = S(\mathcal{A};Y)$ pour prouver le résultat en (4.13). L'idée sera de montrer qu'il existe une transformation unitaire conditionnée sur y qui permet de séparer le registre $\mathcal{B}'$ de $\rho_{X\mathcal{B}\mathcal{B}'}$. Puisque cette transformation ne change pas l'information mutuelle $S(X;\mathcal{B}\mathcal{B}')$, nous conclurons que $\mathcal{B}'$ ne contient aucune information sur X.

Prenons le point de vue de Bob. Une preuve analogue peut être faire pour Alice. Fixons une base orthonormée $\{|k\rangle_{\mathcal{B}'}\}_k$ sur le registre $\mathcal{B}'$. Définissons la transformation, pour

chaque k, conditionnée sur y par

$$U_k|y\rangle_{\mathcal{B}}|f_k^y\rangle_{\mathcal{B}'} = |y\rangle_{\mathcal{B}}|k\rangle_{\mathcal{B}'}. \tag{4.14}$$

Cette transformation unitaire, appliquée à $|\psi\rangle$, un état décorrélé sous sa forme (4.3), produit

$$\left|\tilde{\psi}\right\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}}|y\rangle_{\mathcal{B}} \otimes \sum_k \sqrt{\lambda_k} e^{i\theta(k)} |e_k^x\rangle_{\mathcal{A}'}|k\rangle_{\mathcal{B}'}. \tag{4.15}$$

La trace sur $\mathcal{A}\mathcal{A}'$ de l'état (4.15) ci-haut donne la matrice

$$\begin{aligned} \rho_{\mathcal{B}\mathcal{B}'} &= \mathrm{tr}_{\mathcal{A}\mathcal{A}'}\left(\left|\tilde{\psi}\right\rangle\!\!\left\langle\tilde{\psi}\right|\right) \\ &= \sum_x P_X(x) |\gamma_x\rangle\!\langle\gamma_x|_{\mathcal{B}} \otimes \sum_k \lambda_k |k\rangle\!\langle k|_{\mathcal{B}'} \\ &= \sum_x P_X(x) \rho_{\mathcal{B}}^x \otimes \sigma_{\mathcal{B}'} \end{aligned} \tag{4.16}$$

où $|\gamma_x\rangle_{\mathcal{B}} = \sum_y \sqrt{P_{X,Y}(y|x)} e^{i\theta(x,y)} |y\rangle_{\mathcal{B}}$. Par le lemme 2.4,

$$\begin{aligned} S(\mathcal{B}\mathcal{B}')_\psi &= S(\mathcal{B}\mathcal{B}')_{\tilde{\psi}}, \\ S(\mathcal{B})_\psi &= S(\mathcal{B})_{\tilde{\psi}}, \\ S(\mathcal{B}\mathcal{B}'|X)_\psi &= S(\mathcal{B}\mathcal{B}'|X)_{\tilde{\psi}}, \\ S(\mathcal{B}|X)_\psi &= S(\mathcal{B}|X)_{\tilde{\psi}} \end{aligned} \tag{4.17}$$

sont invariants puisque $|\tilde{\psi}\rangle$ est obtenu en appliquant une transformation unitaire sur $|\psi\rangle$ agissant sur le registre $\mathcal{B}'$ conditionné sur $\mathcal{B}$. La séparabilité de $\rho_{\mathcal{B}\mathcal{B}'}$ en (4.16) implique que

$$S(\mathcal{B}\mathcal{B}')_{\tilde{\psi}} = S(\mathcal{B})_{\tilde{\psi}} + S(\mathcal{B}')_{\tilde{\psi}}$$

$$S(\mathcal{B}\mathcal{B}'|X)_{\tilde{\psi}} = S(\mathcal{B}|X)_{\tilde{\psi}} + S(\mathcal{B}'|X)_{\tilde{\psi}} = S(\mathcal{B}|X)_{\tilde{\psi}} + S(\mathcal{B}')_{\tilde{\psi}}. \tag{4.18}$$

En utilisant les équations (4.17), (4.18) et la définition de l'information mutuelle quantique, nous pouvons conclure que

$$\begin{aligned} S(X;\mathcal{B}\mathcal{B}')_\psi &= S(\mathcal{B}\mathcal{B}')_\psi - S(\mathcal{B}\mathcal{B}'|X)_\psi \\ &= S(\mathcal{B}\mathcal{B}')_{\tilde{\psi}} - S(\mathcal{B}\mathcal{B}'|X)_{\tilde{\psi}} \\ &= S(\mathcal{B})_{\tilde{\psi}} + S(\mathcal{B}')_{\tilde{\psi}} - S(\mathcal{B}|X)_{\tilde{\psi}} - S(\mathcal{B}')_{\tilde{\psi}} \\ &= S(\mathcal{B})_{\tilde{\psi}} - S(\mathcal{B}|X)_{\tilde{\psi}} \\ &= S(\mathcal{B})_\psi - S(\mathcal{B}|X)_\psi \\ &= S(X;\mathcal{B})_\psi. \end{aligned}$$

□

Si un état correct a la propriété qu'un échange entre Alice et Bob de sous-systèmes de $\mathcal{A}'$ et $\mathcal{B}'$ rend leur état décorrélé, alors la fuite d'information doit être plus grande ou égale dans la configuration avant l'échange. Par l'échange de sous-systèmes, nous voulons dire qu'Alice et Bob envoient, par un canal quantique sans bruit, une partie des qubits de leur registre auxiliaire à l'autre participant.

Lemme 4.2. *Soit $|\psi\rangle$ un état décorrélé. Considérons $\mathcal{S} \subseteq \mathcal{A}'$ et $\mathcal{R} \subseteq \mathcal{B}'$, deux sous-ensembles des registres $\mathcal{A}'$ et $\mathcal{B}'$. L'état $|\phi\rangle$ est obtenu par l'échange de $\mathcal{S}$ et $\mathcal{R}$ entre Alice et Bob. Ainsi, $\forall \mathcal{R}, \mathcal{S}$ on a que*

$$\Delta_\phi(P_{X,Y}) \geq \Delta_\psi(P_{X,Y}). \tag{4.19}$$

Démonstration. Par le théorème (2.5) tout état $|\phi\rangle$ satisfait

$$\begin{aligned} S(X;\mathcal{B}\mathcal{B}')_\phi \geq S(X;\mathcal{B})_\phi = S(X;\mathcal{B})_\psi \\ S(\mathcal{A}\mathcal{A}';Y)_\phi \geq S(\mathcal{A};Y)_\phi = S(\mathcal{A};Y)_\psi \end{aligned}$$

puisque la trace partielle constitue une opération quantique. De plus, puisque la différence entre $|\psi\rangle$ et $|\phi\rangle$ survient dans les registres auxiliaires, $S(X;\mathcal{B})$ est identique pour les deux états. Ainsi, par le lemme (4.13) et par la définition de la fuite d'information chez Alice et chez Bob,

$$\begin{aligned}\Delta^A_\phi(P_{X,Y}) = S(\mathcal{A}\mathcal{A}';Y)_\phi - I(X;Y) &\geq S(\mathcal{A};Y)_\psi - I(X;Y) = \Delta^A_\psi(P_{X,Y}) \\ \Delta^B_\phi(P_{X,Y}) = S(X;\mathcal{B}\mathcal{B}')_\phi - I(X;Y) &\geq S(X;\mathcal{B})_\psi - I(X;Y) = \Delta^B_\psi(P_{X,Y}).\end{aligned}$$

Ceci implique donc que

$$\Delta_\phi(P_{X,Y}) \geq \Delta_\psi(P_{X,Y}).$$

□

4.5 Transfert de registre auxiliaire

Dans la section précédente, nous avons établi qu'un état correct ne fuit pas moins d'information qu'un état strict-correct s'il satisfait une certaine propriété. Dans cette section, nous verrons une autre propriété qu'un état correct peut satisfaire qui nous permet d'arriver à une conclusion similaire par rapport à sa fuite d'information.
Pour les états corrects, il existe une asymétrie au niveau de la fuite d'information chez Alice et Bob. Le lemme suivant établit qu'un envoi de registre auxiliaire vers le côté du participant ayant une fuite plus grande ne peut pas faire diminuer la fuite de l'état.

Lemme 4.3. *Prenons $|\psi\rangle$ avec la propriété que $\Delta^B_\psi(P_{X,Y}) \geq \Delta^A_\psi(P_{X,Y})$. Pour tout $\mathcal{S} \subseteq \mathcal{A}'$, un sous-espace de $\mathcal{A}'$ envoyé à Bob pour produire l'enveloppe $|\tilde{\psi}\rangle$, on a que*

$$\Delta_{\tilde{\psi}}(P_{X,Y}) \geq \Delta_\psi(P_{X,Y}). \tag{4.20}$$

L'inégalité ci-haut est vraie également dans le sens inverse où $\Delta^A_\psi(P_{X,Y}) \geq \Delta^B_\psi(P_{X,Y})$ et $|\tilde{\psi}\rangle$ est obtenu par l'envoi d'un sous-système de $\mathcal{B}'$ à Alice.

Démonstration. La preuve fera l'hypothèse que $\Delta_{\psi}^{B}(P_{X,Y}) \geq \Delta_{\psi}^{A}(P_{X,Y})$. Le cas inverse admet une preuve analogue.

Notons les registres auxiliaires suite au transfert de $\mathcal{S}$ par $\tilde{\mathcal{A}} = \mathcal{A}' \setminus \mathcal{S}$ et $\tilde{\mathcal{B}} = \mathcal{B}' \cup \mathcal{S}$. Dans l'état $|\tilde{\psi}\rangle$, Alice possède $\mathcal{A}\tilde{\mathcal{A}}$ et Bob $\mathcal{B}\tilde{\mathcal{B}}$. Puisque Alice n'a plus accès à $\mathcal{S}$, nous traçons sur ce registre pour obtenir

$$\begin{aligned}
\Delta_{\psi}^{A}(P_{X,Y}) &= S(\mathcal{A}\mathcal{A}';Y)_{\psi} - I(X;Y) \\
&= S(\mathcal{A}\tilde{\mathcal{A}}\mathcal{S};Y)_{\psi} - I(X;Y) \\
&\geq S(\mathcal{A}\tilde{\mathcal{A}};Y)_{\tilde{\psi}} - I(X;Y) \\
&= \Delta_{\tilde{\psi}}^{A}(P_{X,Y}).
\end{aligned}$$

Puisque l'information mutuelle quantique est monotone sous la trace partielle, Alice diminue sa fuite d'information en envoyant $\mathcal{S}$ à Bob. Ceci implique aussi que du côté de ce dernier

$$\begin{aligned}
\Delta_{\psi}^{B}(P_{X,Y}) &= S(X;\mathcal{B}\mathcal{B}')_{\psi} - I(X;Y) \\
&\leq S(X;\mathcal{B}\mathcal{B}'\mathcal{S})_{\psi} - I(X;Y) \\
&= S(X;\mathcal{B}\tilde{\mathcal{B}})_{\tilde{\psi}} - I(X;Y) \\
&= \Delta_{\tilde{\psi}}^{B}(P_{X,Y}).
\end{aligned}$$

Le transfert de $\mathcal{S}$ a donc pour effet d'augmenter la fuite de Bob et de réduire celle d'Alice. L'inégalité $\Delta_{\tilde{\psi}}^{B}(P_{X,Y}) \geq \Delta_{\tilde{\psi}}^{A}(P_{X,Y})$ s'applique donc pour $|\tilde{\psi}\rangle$. Nous concluons alors que

$$\Delta_{\tilde{\psi}}(P_{X,Y}) = \Delta_{\tilde{\psi}}^{B}(P_{X,Y}) \geq \Delta_{\psi}^{B}(P_{X,Y}) = \Delta_{\psi}(P_{X,Y}).$$

□

Le prochain résultat est une conséquence directe du lemme 4.3.

Lemme 4.4. *Soit $|\tilde{\psi}\rangle$ un état correct qui exhibe la propriété suivante : il existe un sous-système $\mathcal{S} \subseteq \mathcal{A}'$, ou $\mathcal{S} \subseteq \mathcal{B}'$, tel que si $\mathcal{S}$ est échangé entre Alice et Bob , l'état produit, $|\psi\rangle$, est strict-correct. Alors,*

$$\Delta_{\tilde{\psi}}(P_{X,Y}) \geq \Delta_{\psi}(P_{X,Y}). \tag{4.21}$$

Démonstration. L'idée est de prendre l'état final $|\psi\rangle$ et d'argumenter que, par le lemme 4.3, le renvoi de $\mathcal{S}$ doit faire augmenter la fuite d'information. Supposons que le sous-système $\mathcal{S}$ est envoyé par Alice. La preuve est identique dans le sens inverse.
Puisque l'échange entre Alice et Bob d'un système $\mathcal{S}$ produit un état strict-correct $|\psi\rangle$, il satisfait $S(X;\mathcal{B}\mathcal{B}')_{\psi} = S(\mathcal{A}\mathcal{A}';Y)_{\psi}$. Le renvoi de $\mathcal{S}$ de Bob à Alice doit reproduire l'état initial, $|\tilde{\psi}\rangle$. Nous pouvons appliquer le lemme (4.3) car $|\psi\rangle$ satisfait la condition et conclure que

$$\Delta_{\tilde{\psi}}(P_{X,Y}) \geq \Delta_{\psi}(P_{X,Y}).$$

□

Illustrons ce résultat par un exemple.

Exemple 4.1. *Soit l'enveloppe pour la primitive $P_{\mathsf{X},\mathsf{Y}}$ suivante :*

$$\left|\tilde{\psi}\right\rangle_{\mathcal{A}\mathcal{B}\mathcal{A}'} = \sum_{x,y} \sqrt{P_{\mathsf{X},\mathsf{Y}}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}} \otimes |y\rangle_{\mathcal{A}'}.$$

Alice a une copie de y dans son registre auxiliaire. Si elle envoit $\mathcal{A}'$ à Bob, ils obtiennent l'enveloppe

$$|\psi\rangle_{\mathcal{A}\mathcal{B}\mathcal{B}'} = \sum_{x,y} \sqrt{P_{\mathsf{X},\mathsf{Y}}(x,y)} e^{i\theta(x,y)} |x\rangle_{\mathcal{A}} |y\rangle_{\mathcal{B}} \otimes |y\rangle_{\mathcal{B}'}.$$

Bob a maintenant en main une copie de y qui, intuitivement, ne devrait pas lui permettre

d'obtenir plus d'information qu'en ayant seulement $\mathcal{B}$. Si on trace sur $\mathcal{A}$ et $\mathcal{B}$, on observe

$$\rho_{\mathcal{B}'} = \sum_{x,y} P_{\mathsf{X},\mathsf{Y}}(x,y)|y\rangle\langle y|_{\mathcal{B}'} = \sum_{y} P_{\mathsf{Y}}(y)|y\rangle\langle y|_{\mathcal{B}'}.$$

Conditionné sur x et y l'état dans $\mathcal{B}'$ est

$$\rho_{\mathcal{B}'}^{x,y} = |y\rangle\langle y|_{\mathcal{B}'} = \rho_{\mathcal{B}'}^{y}.$$

Ainsi,

$$S(\mathcal{B}'|XY) = S(\mathcal{B}'|Y)$$

qui, par la condition 3 du lemme 3.1, implique que $|\psi\rangle$ est strict-correct. Puisque $|\tilde{\psi}\rangle$ exhibe la condition du lemme 4.4, il doit fuire plus d'information que $|\psi\rangle$.

4.6 Résumé

Dans ce chapitre, les états corrects ont étés introduits. Ceux-ci sont le produit de la relaxation de la condition sur la fuite dans le cas honnête des états stricts-corrects. Nous avons introduit également l'avantage qui est une mesure de dépendance des registres auxiliaires sur les sorties de la primitive. En utilisant cette mesure, nous avons pu démontrer que la fuite d'information est une quantité continue. Finalement, nous avons démontré que les états corrects satisfaisant certaines conditions ne fuient pas moins d'information que des enveloppes régulières.

CHAPITRE 5

ANALYSE NUMÉRIQUE DE LA FUITE D'INFORMATION

Les conditions énoncées dans le chapitre précédent ne s'appliquent pas à tout les états corrects. En effet, il est possible de construire des enveloppes qui ne satisfont pas les propriétés des lemmes (4.2) et (4.4). Dans ce chapitre, la fuite d'information d'exemples d'états sera calculée. Nous démontrerons des états qui fuient moins d'information que les enveloppes régulières pour la primitive de transfert équivoque de Rabin.

5.1 Méthodologie

Nous décrivons rapidement le code MATLAB qui est à l'annexe I. La routine prend en entrée une description numérique de l'enveloppe exprimée dans la base calculatoire. Les fuites d'Alice et de Bob sont calculées en utilisant les définitions de l'information mutuelle et de l'entropie conditionnelle quantique. Par exemple, la fuite d'Alice est obtenue en calculant de l'entropie de Von Neumann.

$$\begin{aligned}
\Delta_{\psi}^{A}(P_{\mathsf{X},\mathsf{Y}}) &= S(\mathcal{A}\mathcal{A}';Y) - I(X;Y) \\
&= S(\mathcal{A}\mathcal{A}') + H(Y) - S(\mathcal{A}\mathcal{A}'Y) - I(X;Y) \\
&= S(\mathcal{A}\mathcal{A}') - S(\mathcal{A}\mathcal{A}'Y) - H(X) + H(XY).
\end{aligned}$$

Pour calculer l'entropie, le code diagonalise la matrice densité puis calcule l'entropie de Shannon des valeurs propres. Finalement, la mesure de X et Y est obtenue en appliquant le projecteur approprié est en calculant la trace partielle. Cette routine permet d'obtenir la fuite d'information d'Alice et de Bob et produit en sortie le maximum des deux.

5.2 Transfert équivoque d'un parmi deux

Le transfert équivoque d'un parmi deux est une tâche où Alice envoie deux messages, $x_0, x_1 \in \{0,1\}$, et Bob reçoit l'un des deux avec probabilité $1/2$ chacun. Il apprend lequel des deux par un bit de sélection s. Cette primitive, développée par Even et al. [12], fut démontrée complète pour le calcul à deux parties par Kilian [17]. Son intérêt de recherche est alors justifié par sa puissance de calcul.

Comme nous voulons interpréter cette primitive dans le modèle QHMC, nous prenons $x_0, x_1, s \in_R \{0,1\}$ uniformément et Alice reçoit ces deux messages comme sortie du protocole. La distribution de probabilité est la suivante :

$$P^{OT}_{X,Y}((x_0,x_1),(s,y)) = \begin{cases} \frac{1}{8} & \text{si } y = x_s \\ 0 & \text{sinon.} \end{cases}$$

Nous noterons $|x_0,x_1\rangle_{\mathcal{A}}$ pour la partie d'Alice et $|s,y\rangle_{\mathcal{B}}$ pour Bob. Une enveloppe de cette primitive aura donc la forme

$$\begin{aligned} |OT\rangle = \frac{1}{2\sqrt{2}}\Big[& e^{i\theta(00,00)}|00\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} \otimes |\phi^{00,00}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(00,10)}|00\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} \otimes |\phi^{00,10}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(01,00)}|01\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} \otimes |\phi^{01,00}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(01,11)}|01\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}} \otimes |\phi^{01,11}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(10,01)}|10\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} \otimes |\phi^{10,01}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(10,10)}|10\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} \otimes |\phi^{10,10}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(11,01)}|11\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} \otimes |\phi^{11,01}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(11,11)}|11\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}} \otimes |\phi^{11,11}\rangle_{\mathcal{A}'\mathcal{B}'}\Big]. \end{aligned} \tag{5.1}$$

Salvail et al. [26] démontrent que pour cette primitive, le minimum est atteint par une enveloppe régulière $|OT^*\rangle$ où la fonction de phase $\theta(x,y) = c, \forall(x,y)$, où c est une

constante. Les auteurs calculent également la fuite d'information et obtiennent

$$\Delta_{OT^*}(P_{X,Y}) = \frac{1}{2}. \tag{5.2}$$

Dans les sections suivantes, nous ferons la comparaison de la fuite d'information d'états corrects avec la valeur en (5.2).

5.2.1 Phase non triviale

Nous utilisons, dans cette section, des phases différentes pour chaque terme et choisissons arbitrairement que

$$\theta(x,y) = \begin{cases} \frac{\pi}{2} & \text{si } (x,y) = (00,00) \\ \frac{\pi}{3} & \text{si } (x,y) = (01,00) \\ \frac{\pi}{4} & \text{si } (x,y) = (00,10) \\ \frac{\pi}{5} & \text{si } (x,y) = (10,01) \\ \frac{\pi}{6} & \text{si } (x,y) = (01,11), (10,10) \text{ ou } (11,01) \\ \frac{\pi}{8} & \text{sinon.} \end{cases}$$

L'état ainsi généré est

$$\begin{aligned} \left|OT^1\right\rangle = \frac{1}{2\sqrt{2}}\Big[& e^{i\pi/2}|00\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} + e^{i\pi/4}|00\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} + e^{i\pi/3}|01\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} + e^{i\pi/6}|01\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}} \\ & + e^{i\pi/5}|10\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} + e^{i\pi/6}|10\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} + e^{i\pi/6}|11\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} + e^{i\pi/8}|11\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}}\Big]. \end{aligned}$$

En roulant le code dans l'annexe I, nous obtenons

$$\Delta_{OT^1}(P_{X,Y}) = 0.5053 \geq \frac{1}{2}. \tag{5.3}$$

Cet état fuit plus que l'état en (5.2) comme prévu.

5.2.2 États distinguables

Les registres auxiliaires peuvent être utilisés pour aider à distinguer le résultat de l'autre participant. Par exemple, définissons l'état

$$|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle.$$

L'enveloppe que nous analyserons est la suivante :

$$\begin{aligned}
\left|OT^{\theta}\right\rangle = \frac{1}{2\sqrt{2}}\Big[& |00\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\
& +|00\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} \otimes |\theta\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\
& +|01\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|\theta\rangle_{\mathcal{B}'} \\
& +|01\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}} \otimes |\theta\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\
& +|10\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\
& +|10\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} \otimes |\theta\rangle_{\mathcal{A}'}|\theta\rangle_{\mathcal{B}'} \\
& +|11\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|\theta\rangle_{\mathcal{B}'} \\
& +|11\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}} \otimes |\theta\rangle_{\mathcal{A}'}|\theta\rangle_{\mathcal{B}'}\Big].
\end{aligned}$$

L'intérêt ce cette enveloppe est que pour chaque (x, y) mesuré, Alice et Bob observe une mixture équiprobable pour le résultat de son partenaire. Avec ces états dans les registres auxiliaires, ils ont la possibilité de distinguer partiellement cette mixture.

Si Alice et Bob s'échangent $\mathcal{A}'$ et $\mathcal{B}'$ respectivement, l'état devient décorrélé. En effet, chaque état dans les registres auxiliaires ne sont dépendant que de x ou de y. Ainsi, la fuite est plus grande que 0.5 pour toute valeur de θ possible. Les données numériques sont tabulées ci-bas.

Si $\theta = 0$, l'état dans $\mathcal{A}'$ et $\mathcal{B}'$ est complètement séparable et l'enveloppe est stricte-correcte. À l'autre extrême, si $\theta = \pi/2$, alors $|\theta\rangle = |1\rangle$ et les états dans les registres auxiliaires sont parfaitement distinguable. Dans ce cas, Alice et Bob peuvent déterminer

θ	0	$\pi/4$	$\pi/2$
$\Delta_{OT^\theta}(P_{X,Y})$	0.5000 bit	0.6773 bit	1.000 bit

Tableau 5.I – La fuite d'information de $|OT^\theta\rangle$ pour des valeurs de θ.

entièrement le résultat classique de l'autre.

5.2.3 Paire EPR

Au lieu d'utiliser des états qui ne sont pas intriqués entre Alice et Bob, nous leur donnerons des paires EPR dans leurs registres auxiliaires. L'état est

$$\begin{aligned}\left|OT^{EPR}\right\rangle = \frac{1}{2\sqrt{2}}\Big[&|00\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} \otimes \left|\Psi^+\right\rangle_{\mathcal{A}'\mathcal{B}'} \\ &+|00\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} \otimes \left|\Phi^+\right\rangle_{\mathcal{A}'\mathcal{B}'} \\ &+|01\rangle_{\mathcal{A}}|00\rangle_{\mathcal{B}} \otimes \left|\Psi^+\right\rangle_{\mathcal{A}'\mathcal{B}'} \\ &+|01\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}} \otimes \left|\Phi^+\right\rangle_{\mathcal{A}'\mathcal{B}'} \\ &+|10\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} \otimes \left|\Psi^+\right\rangle_{\mathcal{A}'\mathcal{B}'} \\ &+|10\rangle_{\mathcal{A}}|10\rangle_{\mathcal{B}} \otimes \left|\Phi^+\right\rangle_{\mathcal{A}'\mathcal{B}'} \\ &+|11\rangle_{\mathcal{A}}|01\rangle_{\mathcal{B}} \otimes \left|\Psi^+\right\rangle_{\mathcal{A}'\mathcal{B}'} \\ &+|11\rangle_{\mathcal{A}}|11\rangle_{\mathcal{B}} \otimes \left|\Phi^+\right\rangle_{\mathcal{A}'\mathcal{B}'}\Big].\end{aligned}$$

En roulant la routine MATLAB, la fuite d'information calculée est

$$\Delta_{OT^{EPR}}(P_{X,Y}) = \frac{1}{2}$$

comme pour les enveloppes régulières. Un fait intéressant de $|OT^{EPR}\rangle$ est que c'est lui-même un état strict-correct. Les paires EPR parfaites ne semblent donc pas permettre une fuite différente que celle de l'enveloppe régulière en (5.2).

5.3 Transfert équivoque de Rabin

Le transfert équivoque original, proposé par Rabin en 1981 [20], sert à échanger un secret entre Alice et Bob. De façon similaire à la primitive dans la section 5.2, Alice envoie une chaîne de bits x à Bob. Avec probabilité $1/2$, Bob reçoit un symbole spécial, $\perp$, ou la chaîne x. Cette primitive a été démontrée équivalente à 1-2-OT par Crépeau [9]. Elle est ainsi complète pour le calcul à deux parties par transitivité.

La définition probabiliste de la primitive est la suivante : Soit $x \in_R \{0,1\}^r$ et $y \in_R \{0,1\}^r \cup \{\perp\}$, alors

$$P_{X,Y}^{ROT^r}(x,y) = \begin{cases} \frac{1}{4} & \text{si } y = x \text{ ou } y = \perp \\ 0 & \text{sinon.} \end{cases} \tag{5.4}$$

Pour l'analyse numérique, nous fixerons $r = 1$. Ainsi, Alice n'envoie qu'un seul bit. Une enveloppe qui réalise cette primitive a comme forme générale

$$\begin{aligned} |ROT\rangle = \frac{1}{2}\Big[& e^{i\theta(0,0)}|0\rangle_{\mathcal{A}}|0\rangle_{\mathcal{B}} \otimes |\phi^{0,0}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(0,\perp)}|0\rangle_{\mathcal{A}}|\perp\rangle_{\mathcal{B}} \otimes |\phi^{0,\perp}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(1,1)}|1\rangle_{\mathcal{A}}|1\rangle_{\mathcal{B}} \otimes |\phi^{1,1}\rangle_{\mathcal{A}'\mathcal{B}'} \\ & + e^{i\theta(1,\perp)}|1\rangle_{\mathcal{A}}|\perp\rangle_{\mathcal{B}} \otimes |\phi^{1,\perp}\rangle_{\mathcal{A}'\mathcal{B}'} \Big]. \end{aligned}$$

Salvail et al. [26] démontrent que la fuite d'information de toute enveloppe régulière $|ROT^*\rangle$ ne dépend pas de la fonction de phase. La fuite est

$$\Delta_{ROT^*}(P_{X,Y}) \geq H_2\left(\frac{1}{4}\right) - \frac{1}{2} \approx 0.3112.$$

5.3.1 États distinguables

Comme à la section 5.2.2, nous analyserons la fuite d'un état ayant des registres auxiliaires distinguables. Soit

$$|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle.$$

Nous utiliserons le même angle du côté d'Alice et de Bob. L'enveloppe analysée est

$$\begin{aligned}\left|ROT^{\theta}\right\rangle = \frac{1}{2}\Big[& |0\rangle_{\mathcal{A}}|0\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\ & +|0\rangle_{\mathcal{A}}|\perp\rangle_{\mathcal{B}} \otimes |\theta\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\ & +|1\rangle_{\mathcal{A}}|1\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|\theta\rangle_{\mathcal{B}'} \\ & +|1\rangle_{\mathcal{A}}|\perp\rangle_{\mathcal{B}} \otimes |\theta\rangle_{\mathcal{A}'}|\theta\rangle_{\mathcal{B}'}\Big].\end{aligned}$$

Contrairement à la fuite d'information pour la primitive à la section 5.1, lorsque l'état n'est plus strict-correct, nous observons une asymétrie entre la fuite d'Alice et de Bob. Ci-dessous sont les résultats tabulés.

θ	0	$\pi/4$	$\pi/2$
$\Delta^{A}_{ROT^{\theta}}(P_{X,Y})$	0.3112 bit	0.6416 bit	1.0000 bit
$\Delta^{B}_{ROT^{\theta}}(P_{X,Y})$	0.3112 bit	0.3412 bit	0.5000 bit

Tableau 5.II – La fuite d'information de $\left|ROT^{\theta}\right\rangle$ pour des valeurs de θ.

5.3.2 États distinguables avec angles désynchronisés

Reprenons l'état de la section précédente, mais permettons un angle θ_1 chez Alice et θ_2 chez Bob. On obtient

$$\begin{aligned} |ROT'\rangle = \frac{1}{2}\Big[& |0\rangle_{\mathcal{A}}|0\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\ & +|0\rangle_{\mathcal{A}}|\perp\rangle_{\mathcal{B}} \otimes |\theta_1\rangle_{\mathcal{A}'}|0\rangle_{\mathcal{B}'} \\ & +|1\rangle_{\mathcal{A}}|1\rangle_{\mathcal{B}} \otimes |0\rangle_{\mathcal{A}'}|\theta_2\rangle_{\mathcal{B}'} \\ & +|1\rangle_{\mathcal{A}}|\perp\rangle_{\mathcal{B}} \otimes |\theta_1\rangle_{\mathcal{A}'}|\theta_2\rangle_{\mathcal{B}'}\Big]. \end{aligned} \tag{5.5}$$

Contrairement à tous les résultats numériques de ce chapitre, cet état parvient à battre la borne en (5.3). La figure ci-dessous illustre en blanc les valeurs de θ_1 et de θ_2 qui ont une fuite plus grande ou égale à 0.3112. La région foncée représente des états pour qui la fuite est sous cette valeur.

Il existe donc une enveloppe qui ne se retrouve pas parmi les enveloppes régulières qui, malgré cela, bat le minimum atteint par ces dernières. La figure ci-dessous affiche la zone d'intérêt de façon plus détaillée.

L'état $|ROT^{id}\rangle$ qui atteint le minimum numérique (dans la région noire) pour les états ayant la forme en (5.5) a comme angles

$$\begin{aligned} \theta_1 &= 0.1509 \\ \theta_2 &= 0.2301. \end{aligned}$$

La fuite de cet état est

$$\Delta_{ROT^{id}}(P_{X,Y}) = 0.3069.$$

L'existence d'un minimum qui se produit par un état qui n'est pas strict-correct soulève une question importante. Alice et Bob ont-ils avantage à investir dans l'information accessible dans le cas honnête pour améliorer la fuite dans le pire cas ? Puisque $|ROT^{id}\rangle$

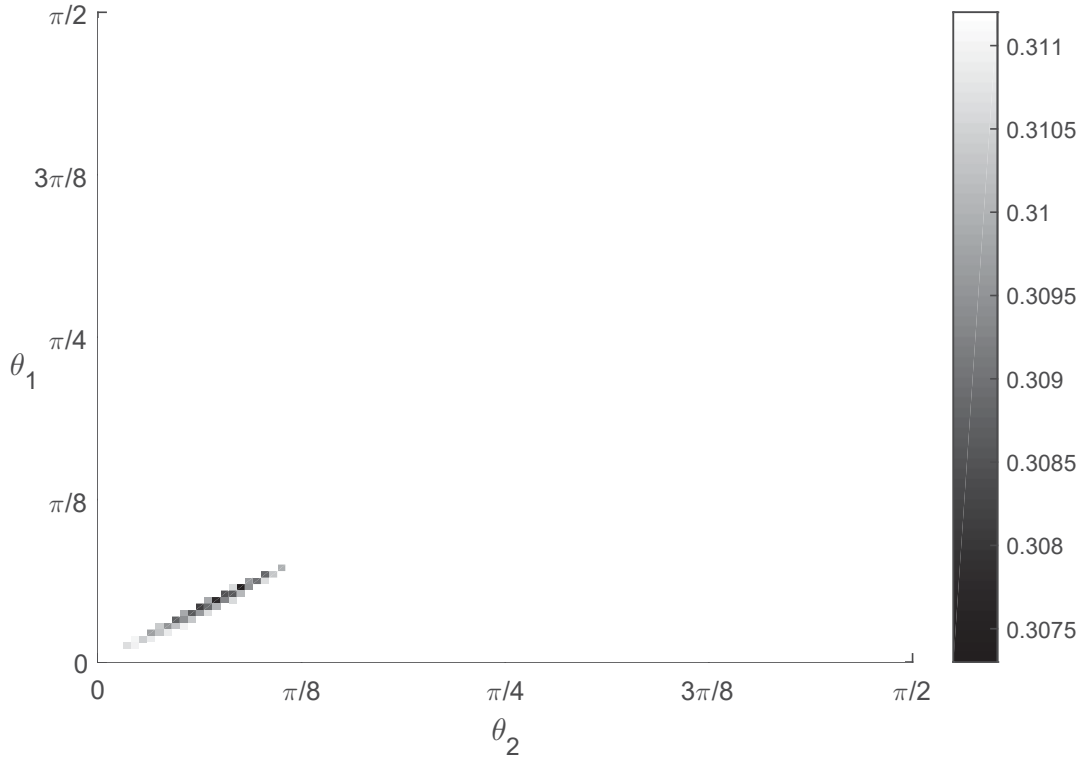

Figure 5.1 – Fuite d'information pour toutes les valeurs de θ_1 et θ_2.

n'est pas strict-correct, nous savons que

$$S(X;Y\mathcal{B}') > I(X;Y)$$

ou

$$S(X\mathcal{A}';Y) > I(X;Y).$$

En d'autres mots, en adoptant un protocole qui produit la purification $|ROT^{id}\rangle$, ils réduisent l'information accessible aux participants malhonnêtes, mais augmentent l'information accessible aux participants honnêtes. Dans le premier cas, la réduction en fuite d'information est 0.0044 bit alors qu'ils doivent investir 0.0506 bit dans le deuxième cas. $|ROT^{id}\rangle$ est le premier exemple à exhiber une telle propriété, toutes les purifications explorées jusqu'ici fuyaient autant d'information ou plus que $1/2$.

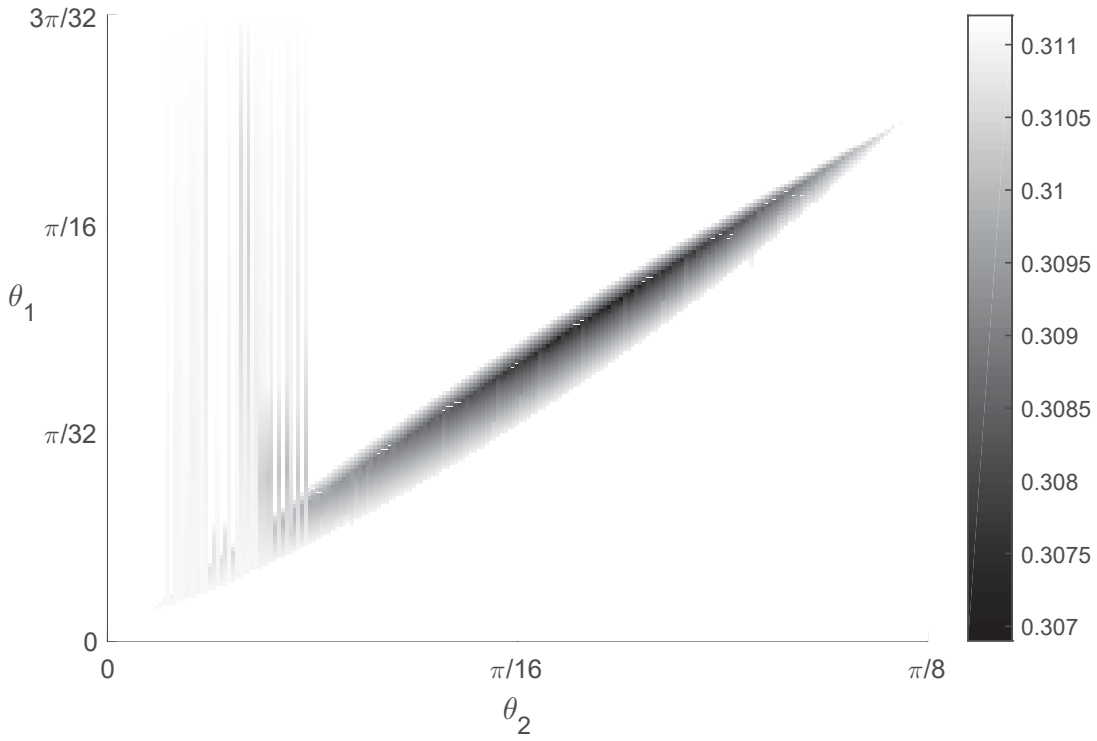

Figure 5.2 – Agrandissement de la région où la fuite d'information bat la borne inférieure des états stricts-corrects.

Cette différence entre l'investissement et la diminution en fuite d'information soulève une question intéressante : existe-t-il des états corrects qui fuient moins d'information que les enveloppes régulières et qui requiert moins d'investissement dans le cas honnête que dans le cas malhonnête ? Dans certain cas, un état qui fuit moins d'information dans le pire cas, tel que $|ROT^{id}\rangle$ fait, est avantageux à réaliser. Par contre, si selon la métrique qui assigne un poids équivalent à la fuite d'information dans le cas honnête et malhonnête, alors un état strict-correct reste la meilleure option. Ce questionnement laisse place à une recherche plus approfondie des états corrects, particulièrement pour des primitives classiques différentes.

5.4 Résumé

Dans ce dernier chapitre, l'analyse numérique de la fuite d'information des primitives 1-2-OT et ROT a été réalisée à l'aide d'une routine MATLAB. Celle-ci a révélé un état qui permet de fuir moins d'information que le minimum atteint pour les enveloppes régulières de la primitive ROT. Ce résultat démontre qu'il existe des purifications qui permettent à Alice et Bob d'investir de la fuite dans le cas honnête, mais en échange, diminuent la fuite dans le pire cas.

CONCLUSION

Nous avons introduit le concept d'avantage pour les états corrects qui réalisent une primitive cryptographique. Cette notion mène à la conclusion que la fuite d'information est continue selon la dépendance des registres auxiliaires avec les variables classiques d'Alice et de Bob.

Nous avons ensuite démontré que les états corrects qui admettent une configuration décorrélée sous échange de registres auxiliaires fuient plus d'information dans leur configuration originale. Nous avons démontré le même résultat mais pour les états qui admettent une configuration stricte-correcte sous envoi unidirectionnel de registres auxiliaires. De ce fait, nous avons montré que les résultats de Salvail et al. [26] s'étendent à une catégorie d'états corrects, répondant alors partiellement à la question ouverte qu'ils posent dans leur publication originale.

Nous avons finalement soulevé quelques exemples de réalisations quantiques pour les primitives de transfert 1 parmi 2 et du transfert de Rabin. Nous avons calculé numériquement la fuite d'information pour ces réalisations et nous démontrons qu'il est possible de fuir moins d'information que le minimum atteint parmi les enveloppes régulières.

Avenues de recherche

La découverte des états qui fuient moins d'information que les enveloppes régulières ouvre la porte à la recherche de réalisation qui optimise l'investissement entre le cas honnête et le cas malhonnête. Il est possible qu'il existe des états tels que la diminution de fuite d'information dans le pire cas est plus grande que l'augmentation de la fuite pour des participants honnêtes.

De plus, il reste à explorer les états corrects de façon à déterminer s'il existe un minimum absolu pour la fuite d'information. Les exemples numériques ne sont pas généraux et une analyse plus en profondeur est nécessaire.

Finalement, la fuite d'information s'applique à des primitives à deux partis. Il reste à

démontré s'il existe des monotones quantiques lorsque les protocoles sont réalisés par n participants, pour tout n plus grand que 2.

BIBLIOGRAPHIE

[1] Robert Alicki et Mark Fannes. Continuity of quantum conditional information. *Journal of Physics A : Mathematical and General*, 37(5):L55, 2004.

[2] John S Bell. On the einstein podolsky rosen paradox, 1964.

[3] Charles H. Bennett et Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. Dans *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.

[4] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres et William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[5] N. J. Cerf et C. Adami. Negative entropy and information in quantum mechanics. *Phys. Rev. Lett.*, 79:5194–5197, Dec 1997. URL `http://link.aps.org/doi/10.1103/PhysRevLett.79.5194`.

[6] N. J. Cerf et C. Adami. Quantum extension of conditional probability. *Phys. Rev. A*, 60:893–897, Aug 1999. URL `http://link.aps.org/doi/10.1103/PhysRevA.60.893`.

[7] Andr'e Chailloux et Iordanis Kerenidis. Optimal quantum strong coin flipping. Dans *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 527–533. IEEE, 2009.

[8] Thomas M Cover et Joy A Thomas. Information theory and statistics. *Elements of Information Theory*, pages 279–335, 1991.

[9] Claude Crépeau. Equivalence between two flavours of oblivious transfers. Dans *Conference on the Theory and Application of Cryptographic Techniques*, pages 350–354. Springer, 1987.

[10] Ivan B Damgård, Serge Fehr, Louis Salvail et Christian Schaffner. Secure identification and qkd in the bounded-quantum-storage model. Dans *Advances in Cryptology-CRYPTO 2007*, pages 342–359. Springer, 2007.

[11] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[12] Shimon Even, Oded Goldreich et Abraham Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, juin 1985. ISSN 0001-0782. URL `http://doi.acm.org/10.1145/3812.3818`.

[13] Serge Fehr et Christian Schaffner. Composing quantum protocols in a classical environment. Dans *Theory of Cryptography*, pages 350–367. Springer, 2009.

[14] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[15] Michał Horodecki, Jonathan Oppenheim et Andreas Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269(1): 107–136, 2007.

[16] J. A. Jones et M. Mosca. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. *The Journal of Chemical Physics*, 109(5): 1648–1653, 1998. URL `http://scitation.aip.org/content/aip/journal/jcp/109/5/10.1063/1.476739`.

[17] Joe Kilian. Founding cryptography on oblivious transfer. Dans *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 20–31, 1988. URL `http://doi.acm.org/10.1145/62212.62215`.

[18] Hoi-Kwong Lo et Hoi Fung Chau. Is quantum bit commitment really possible ? *Physical Review Letters*, 78(17):3410, 1997.

[19] D. Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters*, 78:3414–3417, avril 1997.

[20] O Michael. Rabin. how to exchange secrets by oblivious transfer. *Technical reportä TR-81, Aiken Computation Lab, Harvard University*, 1981.

[21] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. *arXiv preprint arXiv :0711.4114*, 2007.

[22] Michele Mosca. Cybersecurity in an era with quantum computers : will we be ready ? Rapport technique, IACR Cryptology ePrint Archive Report 2015/1075, 2015. http ://eprint. iacr. org, 2015.

[23] John Von Neumann. *Mathematical foundations of quantum mechanics*. Numbéro 2. Princeton university press, 1955.

[24] Michael A. Nielsen et Isaac L. Chuang. *Quantum Computation and Quantum Information : 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th édition, 2011. ISBN 1107002176, 9781107002173.

[25] R. L. Rivest, A. Shamir et L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, février 1978. ISSN 0001-0782. URL `http://doi.acm.org/10.1145/359340.359342`.

[26] Louis Salvail, Christian Schaffner et Miroslava Sotáková. On the power of two-party quantum cryptography. Dans *Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security : Advances in Cryptology*, ASIACRYPT '09, pages 70–87, Berlin, Heidelberg, 2009. Springer-Verlag. ISBN 978-3-642-10365-0. URL `http://dx.doi.org/10.1007/978-3-642-10366-7_5`.

[27] Erwin Schrödinger. Quantization as an eigenvalue problem. *Annalen der Physik*, 79(4):361–376, 1926.

[28] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, July 1948. ISSN 0005-8580.

[29] P. W. Shor. Algorithms for quantum computation : discrete logarithms and factoring. Dans *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134, Nov 1994.

[30] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, 41:303–332, janvier 1999.

[31] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013. ISBN 9781139525343. URL `http://dx.doi.org/10.1017/CBO9781139525343`. Cambridge Books Online.

[32] Stefan Wolf et J Wullschleger. Zero-error information and applications in cryptography. Dans *Information Theory Workshop, 2004. IEEE*, pages 1–6. IEEE, 2004.

[33] Stefan Wolf et Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. *Information Theory, IEEE Transactions on*, 54(6): 2792–2797, 2008.

Annexe I

Code MATLAB pour l'analyse numérique

```
function delta = leakage( state, dim )
%%Calcule la fuite de l'etat bien formatte 'state'
%%Retourne la fuite d'alice et de bob

stateDensityMatrix = state*state';
state_xb = zeros(size(stateDensityMatrix));

%%Calcule H(X), H(Y), H(XY) pour I(X;Y)
for i=1:dim(1) %%applique le projecteur x
    POVM_element = Tensor((basis(dim(1),i)*basis(dim(1),i)'), ...
                          eye(dim(2)),eye(dim(3)),eye(dim(4)));
    state_xb = state_xb + mmult(mmult(POVM_element, ...
                          stateDensityMatrix,1),POVM_element',1);
end

state_xy = zeros(size(stateDensityMatrix));
state_ay = zeros(size(stateDensityMatrix));

for i=1:dim(2) %%applique le projecteur y
    POVM_element = Tensor(eye(dim(1)),(basis(dim(2),i)* ...
                    basis(dim(2),i)'),eye(dim(3)),eye(dim(4)));
    state_ay = state_ay + mmult(mmult(POVM_element, ...
                          stateDensityMatrix,1),POVM_element',1);
    state_xy = state_xy + mmult(mmult(POVM_element,state_xb,1), ...
                          POVM_element',1);
end

```

```
28 %%Calcule H(XY), H(X) et H(Y) pour I(X;Y)
29 H_xy = VNent(PartialTrace(state_xy,[3,4],dim));
30 H_x = VNent(PartialTrace(state_xy,[2,3,4],dim));
31 H_y = VNent(PartialTrace(state_xy,[1,3,4],dim));
32 I_xy = H_x + H_y - H_xy;
33
34 %%Calcule S(BB'), S(XBB') pour S(X;BB')
35 H_bb = VNent(PartialTrace(state_xb,[1,3],dim));
36 H_xbb = VNent(PartialTrace(state_xb,3,dim));
37 S_xbb = H_x + H_bb - H_xbb;
38 delta_b = S_xbb - I_xy;
39
40 %%Calcule S(AA'), S(YAA') pour S(Y;AA')
41 H_aa = VNent(PartialTrace(state_ay,[2,4],dim));
42 H_aay = VNent(PartialTrace(state_ay,4,dim));
43
44 S_yaa = H_y + H_aa - H_aay;
45
46 delta_a = S_yaa - I_xy;
47
48 delta = [delta_a,delta_b];
49
50 end
```

```
1 function ei = basis( dim, i )
2 %%Retourne l'element i de la base calculatoire en dimension dim
3 ei = zeros(1,dim)';
4 ei(i) = 1;
5
6 end
```

```
function C = mmult( A,B, laptop )
%MMULT calcule la multiplication matricielle de A et B
if laptop == 1
    [n, m] = size(A);
    C = zeros(n,n);
    if n==m
        for i=1:n
            for j=1:n
                C(i,j) = A(i,:)*B(:,j);
            end
        end
    else
        error('This function only works for square matrices. ...
        Output is null');
    end
else
    C = A*B;
end

end
```