Quantum Coin Flipping and Bit Commitment

Optimal Bounds, Practical Constructions and Computational Security

Thèse présentée au

Laboratoire de Recherche en Informatique, Université Paris Sud

pour obtenir le grade de

Docteur en Informatique

par

André Chailloux

soutenue le 24 juin 2011 devant le jury composé de

Philippe Dague	Président du jury
Louis Salvail	Rapporteur
Ronald de Wolf	Rapporteur
Olivier Bournez	Membre du jury
Serge Massar	Membre du jury
Iordanis Kerenidis	Directeur de thèse

Année 2011 École Doctorale d'Informatique de Paris Sud

Remerciements

J'aimerai tout d'abord remercier mon directeur de thèse Iordanis Kerenidis. C'est grâce à lui que j'ai découvert l'informatique quantique. Sa manière de toujours vouloir trouver une intuititon derrière les résultats, sa manière de vouloir relier différents domaines de l'informatique quantique et son inventivité m'ont appris le métier de chercheur et m'ont donné l'envie de continuer sur cette voie.

J'aimerai égalament remercier mes rapporteurs de thèse; Louis Salvail pour ses conseils avisés et Ronald de Wolf pour m'avoir obligé à rendre certaines parties de ma thèse plus rigoureuses. Je voudrais aussi remercier les membres de mon jury; Philippe Dague pour m'avoir soutenu et encouragé pour la suite de ma carrière de chercheur, Olivier Bournez, avec lequel j'ai fait mon première stage de recherche et dont je garde un excellent souvenir et Serge Massar, avec qui j'ai fait une collaboration fructueuse et grâce auquel j'ai pu étudier le lien entre les primitives cryptographiques quantiques et la non-localité quantique.

J'aimerai également remercier tous les membres de l'équipe Algorithmes et Complexité du LIAFA grâce auxquels j'ai eu des conditions de travail remarquables, en particulier Miklos, Frédéric, Sophie, Adi, Julia, Michel, David.

J'aimerai également remercier tous les chercheurs avec lesquels j'ai pu collaborer ou discuter. Pour n'en citer que quelques uns: Dorit, Maor, Julien, Stefano, Jamie, Bill, Hirotada, Keiji, Nisheeth, Scott, Thomas, Or, Rahul, Salil, Florin.

J'aimerai aussi remercier tous les étudiants que j'ai cotoyé: Loïck, Xavier, Christian, les Marc, les Matthieu, Djamal, Anna, Charles, Laure ainsi que le personnel administratif qui m'a beaucoup aidé dans mes démarches.

Enfin, j'aimerai remercier mes proches, ma famille et mes avis pour tout le soutien qu'ils m'ont apporté durant toutes ces années.

Contents

Chapter 1

Introduction(en français)

1.1 L'informatique quantique

La mécanique quantique est l'une des plus importantes découvertes du siècle dernier en physique théorique. Grâce à la mécanique quantique, nous savons qu'à une très petite échelle, les particules se comportent très différemment de ce que nous pensions auparavant. À cette échelle, les particules possèdent plusieurs états simultanés et sont modifiées lorsqu'elles sont observées. Bien que ces concepts furent développés à la fin des années 1930, de nombreux mystères liés à cette théorie demeurent, en raison de sa nature contre-intuitive. Pourtant, de nombreuses expériences ont confirmé la nature quantique du monde.

Au milieu des années 80, le physicien Richard Feynman eut une idée remarquable : si nous pouvions contrôler les états quantiques de certaines particules, nous pourrions simuler des systèmes physiques quantiques. L'informatique quantique est née de son premier article [Fey82]. L'idée de base est qu'au lieu de travailler avec des bits, qui prennent la valeur 0 ou 1, nous allons travailler avec des bits quantiques, appelés qubits, qui sont des superpositions de bits. Un qubit peut prendre la valeur 0 et 1 simultanémenet avec des coefficients associés.

L'informatique quantique offre nouvelles perspectives. En manipulant des qubits en superposition, nous pourrons être en mesure de faire des calculs en parallèle et résoudre certains problèmes beaucoup plus rapidement qu'en informatique classique. En 1994, Peter Shor a découvert que la factorisation (voir fig Figure 1.1) peut être réalisée en temps polynomial sur un ordinateur quantique [Sho94]. Cela signifie que toutes les applications cryptographiques basées sur la difficulté de la factorisation (y compris l'algorithme RSA) peuvent être brisées en utilisant un ordinateur quantique.

Ce résultat a soulevé un grand intérêt pour le calcul quantique qui est devenu aujourd'hui un sujet de recherche très important et fructueux. Un autre exemple de la supériorité du calcul quantique : Grover a montré que l'on peut trouver un élément dans un ensemble de données de taille n en temps $O(\sqrt{n})$[Gro97] à l'aide d'un ordinateur quantique, au lieu de $O(n)$ pour un ordinateur classique. Cependant, ces algorithmes quantiques sont encore très difficiles à mettre en œuvre car il est difficile de contrôler un grand nombre de qubits simultanément.

Une autre caractéristique importante des états quantiques, est qu'ils perdent leur comportement quantique lorsqu'on les observe. Tant qu'un état quantique

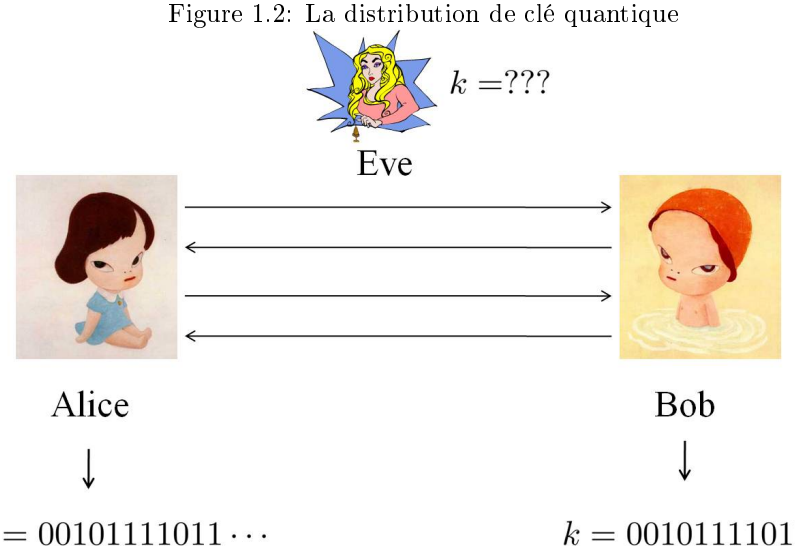
Figure 1.1: Factorisation

- Entrée: n'importe quel nombre $n = p \cdot q$ ou p, q sont des nombres premiers et $p, q \neq 1$
- But: trouver p et q

Par exemple, si $n = 657713791279$, il faut découvrir que $657713791279 = 660661 \cdot 995539$. Généralement, lorsque n est de 100 chiffres (lorsque p, q ont de l'ordre de 50 chiffres), le problème est difficile pour un ordinateur classique, mais pourrait être facilement résolu par un ordinateur quantique.

n'est pas observé, il reste dans une superposition d'états. Mais quand il est observé, il choisit de manière probabiliste l'état dans lequel il se trouve. Cela signifie que les états quantiques changent lorsqu'on les observe. En 1984, Bennett et Brassard [BB84] ont montré comment utiliser ce phénomène quantique pour effectuer une tâche cryptographique : la distribution de clé (figure Figure 1.1), ce qui est impossible à réaliser inconditionnellement en utilisant uniquement des ordinateurs classiques. La cryptographie quantique a depuis été développée dans plusieurs directions et il est déjà possible de mettre en œuvre pratiquement ces protocoles. Le coût et l'efficacité de la cryptographie quantique est aujourd'hui moins bonne que son homologue classique, mais elle devient de plus en plus viable et plusieurs sociétés vendent déjà des dispositifs quantiques.

Figure 1.2: La distribution de clé quantique



Alice et Bob communiquent quantiquement. Leur but est de partager une clé commune k. Ève ne doit pas être en mesure d'obtenir des informations sur la clé k sans qu'Alice et Bob ne le remarquent.

1.2 Primitives cryptographiques

La cryptographie est l'étude et la pratique de la dissimulation d'information. Elle est utilisée dans de très nombreuses applications comme les cartes de paiement, le commerce électronique ou plus simplement par quiconque souhaitant envoyer un courriel sans être espionné. La cryptographie est largement utilisée dans la vie quotidienne.

Si nous avions à analyser et à prouver la sécurité de tous les systèmes cryptographiques séparément, la probabilité de commettre des erreurs serait énorme. Il est plus efficace d'utiliser des blocs de base qui, assemblés, permettent de construire des cryptosystèmes plus complexes. Ces blocs de base sont appelés primitives cryptographiques et vont être étudiés dans cette thèse.

Nous nous intéresserons à certaines primitives cryptographiques fondamentales : le *pile-ou-face*, la *mise-en-gage* de bit, et la *transmission inconsciente*.

Le *pile-ou-face* est une primitive cryptographique qui permet à deux personnes éloignées l'une de l'autre, Alice et Bob, de créer un bit aléatoire qui reste non biaisé, même si l'un des joueurs tente de tricher. Cette primitive a d'abord été proposée par Blum [Blu81] et a depuis trouvé de nombreuses applications dans le calcul sécurisé à deux joueurs.

La primitive de *mise-en-gage* de bit se compose de deux phases: dans la phase de mise-en-gage, Alice s'engage sur un bit b; dans la phase de révélation, Alice révèle ce bit b à Bob. On veut s' assurer de deux choses : que Bob n'ait pas d'informations sur b après la phase de mise-en-gage et qu'Alice ne puisse pas changer d'avis lorsqu'elle révèle b.

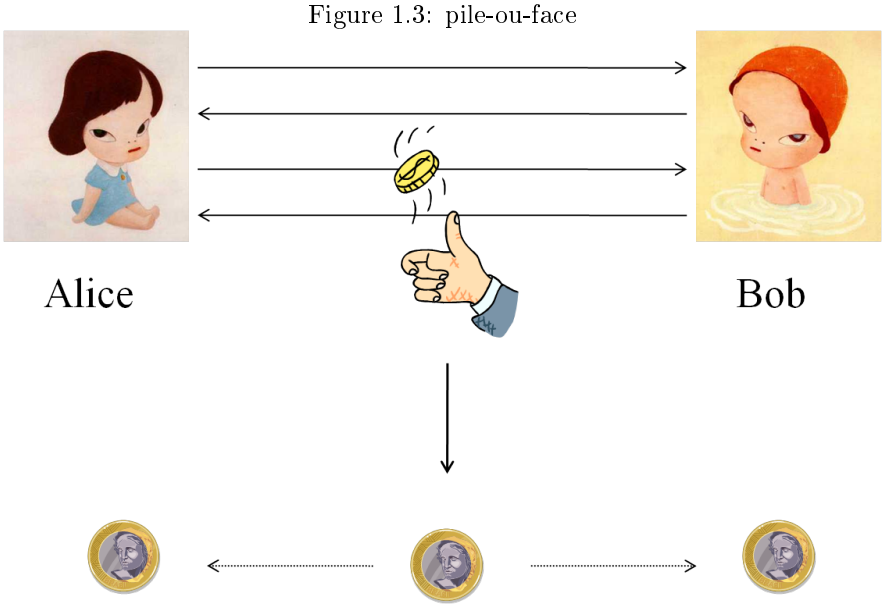
La *transmission inconsciente* est la primitive la plus forte car c'est une primitive universelle pour tout calcul sécurisé à deux joueurs [Rab81, EGL82, Cré87]. Ceci signifie que si on peut effectuer la transmission inconsciente de manière parfaite, alors on peut réaliser tout type de calcul à deux joueurs de manière sécurisée. Nous étudions plus précisément la transmission inconsciente 1-2 aléatoire. À la fin d'un tel protocole, Alice se retrouve avec deux bits aléatoires (x_0, x_1) et se retrouve avec x_b et Bob b pour un choix aléatoire de b. L'objectif du protocole est de veiller à ce que Bob n'ait aucune information sur $x_{\overline{b}}$ et que Alice n'ait aucune information sur b.

En informatique classique, toutes ces primitives sont utilisées pour construire des cryptosystèmes, et l'informatique quantique ne semble pas nécessaire. Cependant, toutes les constructions de ces primitives classiques reposent sur des hypothèses de calcul. Par exemple, il est possible de réaliser (presque) parfaitement un pile ou face en prenant comme hypothèse que la factorisation est un problème difficile. La sécruité de ces primitives en cryptographie classique repose sur des hypothèses de calcul. Nous disons alors que ces primitives sont sécurisées du point de vue calculatoire.

Une notion plus forte de sécurité est la sécurité inconditionnelle. Dans ce cadre, les primitives doivent être sécurisées, même contre un adversaire tout puissant, c'est à dire un joueur qui peut facilement factoriser ou exécuter tout type d'opération. Dans le cadre de la cryptographie classique, nous savons qu'il est impossible d'avoir une sécurité inconditionnelle pour la plupart de ces primitives cryptographiques. Pire, lorsque l'on considère des adversaires tout puissants, nous pouvons dire la chose suivante

Dans tout pile-ou-face , mise-en-gage de bit ou protocole de transmission in-

Figure 1.3: pile-ou-face



Alice and Bob sont loin. Ils veulent tirer à pile ou face mais ne se font pas confiance.

consciente classique, au moins un joueur peut tricher avec une probabilité de 1 *dans le cadre de la sécurité inconditionnelle*

Cela signifie que ces primitives sont impossibles à réaliser dans le modèle de calcul classique de manière inconditionnelle.

1.3 Les limites physiques des primitives cryptographiques quantiques

L'informatique quantique nous donne l'occasion de réétudier la sécurité inconditionnelle en cryptographie. Le premier résultat a été le protocole de distribution quantique de clé de Bennett et Brassard [BB84]. Dès lors, de nombreux travaux ont porté sur la possibilité de réaliser d'autres primitives cryptographiques grâce à l'informatique quantique. Malheureusement, les résultats suivants ont été négatifs. Mayers et Lo, Chau ont prouvé l'impossibilité de la mise-en-gage de bit quantique ainsi que de la transmission inconsciente et par conséquent de tout type de calcul sécurisé à deux joueurs [May97, LC97, DKSW07].

Ces résultats d'impossibilité empêchent la construction de primitives cryptographiques parfaites. Mais il pourrait être possible de construire des primitives cryptographiques quantiques presque parfaites. Aharanov *et al.* [ATVY00] ont d'abord montré comment construire une mise-en-gage de bit quantique imparfaite où la probabilité de tricher est inférieure à $0,9143$. Le meilleur protocole est dû à Ambainis qui a construit un protocole de mise-en-gage de bit (et aussi un pile-ou-face quantique), dans lequel aucun joueur ne peut tricher avec une

probabilité supérieure à $\frac{3}{4}$ [Amb01].

Il existe un protocole de pile-ou-face quantique et un protocole de mise-en-gage de bit quantique dans lequel chaque joueur peut tricher avec une probabilité d'au plus $\frac{3}{4}$.

D'autre part, Kitaev a montré qu'il n'est pas possible de construire des protocoles quantiques de pile-ou-faces avec une probabilité de tricher inférieure à $\frac{1}{\sqrt{2}}$

Dans n'importe quel protocole de mise-en-gage de bit ou de pile-ou-face, au moins un des joueurs peut tricher avec une probabilité de $\frac{1}{\sqrt{2}}$.

On en déduit que les lois de la physique quantique permettent théoriquement de construire un protocole de pile-ou-face avec une probabilité de tricher égale à $\frac{3}{4}$, mais aucun protocole de pile-ou-face n'est physiquement réalisable avec une probabilité de tricher inférieure à $\frac{1}{\sqrt{2}}$, si on suppose que les lois de la physique quantique sont vraies.

Une autre notion de pile-ou-face a été étudiée: le pile-ou-face faible. Dans ce cas, nous voulons faire en sorte qu'Alice ne puisse pas tricher pour que la pièce tombe sur 'PILE' et d'autre part que Bob ne puisse pas tricher pour que la pièce tombe sur 'FACE'. Contrairement au pile-ou-face usuel, Alice peut forcer le résultat 'FACE' avec une probabilité de 1 et Bob peut forcer le résultat 'PILE' avec une probabilité de 1. Après une série de travaux [Moc04, Moc05, Moc07], Mochon a montré comment construire un pile-ou-face faible quantique, qui est presque parfaitement sécurisé. Par opposition à cette notion de pile-ou-face faible, nous appellerons le pile-ou-face standard le pile-ou-face fort. Même pour cette définition faible, il est impossible de construire un tel protocole en informatique classique.

Nous avons amélioré les limites physiques pour des primitives cryptographiques quantiques. Dans le chapitre 4, nous étudions le pile-ou-face quantique. Nous y montrons comment construire un protocole de pile-ou-face quantique avec une probabilité de tricher arbitrairement proche de $\frac{1}{\sqrt{2}}$. De la borne inférieure de Kitaev, nous savons que nos protocoles sont arbitrairement proche de l'optimal. Plus précisément, nous montrons que

Théorème 1 *Pour tout $\varepsilon > 0$, il existe un pile-ou-face fort quantique avec une probabilité de tricher de* $\frac{1}{\sqrt{2}} + \varepsilon$.

Pour montrer ce théorème, nous nous servons du pile-ou-face faible de Mochon. Nous construisons un protocole classique où nous utilisons ce pile-ou-face faible comme un sous-protocole. Cela signifie que la capacité d'effectuer un pile-ou-face quantique fort avec une probabilité de tricher de $\frac{1}{\sqrt{2}}$ vient de la possibilité d'effectuer un pile-ou-face quantique faible (presque) parfait. De manière équivalente, si nous pouvions construire un pile-ou-face faible classiquement alors notre construction donnerait un pile-ou-face classique fort avec une probabilité de tricher de $\frac{1}{\sqrt{2}}$.

Nous étudions ensuite les limites physiques de la mise-en-gage de bit. Avant notre travail, les bornes pour le pile-ou-face quantique et la mise-en-gage de bit quantique étaient les mêmes. On ne savait pas si ces deux primitives avaient la

même borne optimale. Dans le chapitre 5, nous montrons que ce n'est pas le cas. Nous montrons d'abord une meilleure borne inférieure pour la mise-en-gage de bit quantique.

Théorème 2 *Dans tout protocole quantique de mise-en-gage de bit, au moins un des joueurs peut tricher avec une probabilité de* $0,739$.

Ensuite, nous fournissons une limite supérieure correspondante. Nous décrivons un protocole de mise-en-gage de bit qui permet d'obtenir une probabilité de tricher arbitrairement proche de $0,739$.

Théorème 3 *Pour tout* $\varepsilon > 0$*, il existe un protocole quantique de mise-en-gage de bit avec une probabilité de tricher inférieure à* $0,739 + \varepsilon$.

Ce protocole utilise également le pile-ou-face faible de Mochon comme un sous-protocole. Toutefois, ce protocole est quantique même au-delà du sous-protocole. Ceci est en effet nécessaire. Nous montrons que tout protocole classique de mise-en-gage de bit avec la possibilité d'utiliser un pile-ou-face faible (ou même fort) parfait ne peut avoir une probabilité de tricher inférieure à $\frac{3}{4}$.

Théorème 4 *Tout protocole de mise-en-gage de bit classique avec accès à un pile-ou-face faible (ou fort) ne peut pas avoir une probabilité de tricher inférieure à* $\frac{3}{4}$.

Contrairement au cas du pile-ou-face fort qui utilise un pile-ou-face faible et un protocole classique, la mise-en-gage de bit optimale utilise des effets quantiques au-delà du pile-ou-face faible.

Dans le chapitre 6, nous étendons ces résultats à la transmission inconsciente. Nous présentons les premières bornes de transmission inconsciente quantique. Contrairement au pile-ou-face quantique et à la mise-en-gage de bit, nous n'avons pas été en mesure de trouver une borne optimale pour la transmission inconsciente quantique. Nous montrons d'abord une faible borne inférieure pour cette primitive.

Théorème 5 *Dans tout protocole quantique de transmission inconsciente, au moins l'un de joueurs peut tricher avec probabilité supérieure à* $0,58$

Pour démontrer ce théorème, nous réduisons tout protocole de transmission inconsciente à un protocole de mise-en-gage de bit. Nous utilisons ensuite les bornes inférieures de la mise-en-gage quantique pour conclure. Le protocole de mise-en-gage de bit résultant n'a pas les probabilités de tricher que le protocole de transmission inconsciente d'origine, c'est pourquoi la borne inférieure de la transmission inconsciente quantique est moins bonne que la borne inférieure de la mise-en-gage de bit.

On construit ensuite un protocole avec une probabilité de tricher de $\frac{3}{4}$.

Théorème 6 *Il existe un protocole de transmission inconsciente quantique qui permet d'obtenir des probabilités de tricher d'au plus* $\frac{3}{4}$

Les tableaux suivants présentent les anciennes et les nouvelles bornes obtenues dans cette thèse pour les primitives cryptographiques quantiques, pour tout $\varepsilon > 0$.

Anciennes bornes pour les primitives cryptographiques quantiques.

	Borne inférieure	Borne supérieure
pile-ou-face faible	$1/2$	$1/2 + \varepsilon$
pile-ou-face fort	$\frac{1}{\sqrt{2}}$	$3/4$
mise-en-gage de bit	$\frac{1}{\sqrt{2}}$	$3/4$
transmission inconsciente	*	*

*Les bornes pour la transmission inconsciente ont été étudiées dans [SSS09]. Les bornes obtenues sont exprimées en terme d'entropie pour une notion un peu plus forte de la transmission inconsciente. Ces bornes ne sont pas comparables avec les bornes obtenues dans cette thèse

Nouvelles bornes pour les primitives cryptographiques quantiques.

	Borne inférieure	Borne supérieure
pile-ou-face faible	$1/2$	$1/2 + \varepsilon$
pile-ou-face fort	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}} + \varepsilon$
mise-en-gage de bit	$0,739$	$0,739 + \varepsilon$
transmission inconsciente	0,58	$3/4$

1.4 Modèles pratiques pour la cryptographie quantique à deux joueurs

Dans la première partie, nous avons étudié les possibilités et les limites de la cryptographie quantique avec une sécurité inconditionnelle. Nous allons maintenant étudier la mise en œuvre pratique de ces primitives. Ceci a largement été fait pour la distribution de clé quantique ainsi que pour les primitives cryptographiques quantiques mais sans sécurité inconditionnelle. Notre objectif est de mettre en œuvre ces primitives avec une sécurité inconditionnelle. Bien sûr, nos résultats seront plus faibles que ceux obtenus pour la distribution de clé quantique, puisque nous sommes limités par les bornes inférieures décrites précédemment, et donc dans nos protocoles, il y aura toujours une probabilité constante de tricher.

1.4.1 Le modèle indépendant-du-dispositif

Un protocole quantique est dit indépendant-du-dispositif si la fiabilité de sa mise en œuvre peut être garantie sans faire aucune supposition concernant le fonctionnement interne des appareils quantiques utilisés.

Le modèle indépendant-du-dispositif consiste à prendre en compte toutes les défaillances du matériel quantique et les stratégies malicieuses associées, comme, par exemple, celles qui sont exploitées dans [XQL10, LWW$^+$10].

En fait, un protocole indépendant-du-dispositif, en principe, doit rester sécurisé même si les appareils de mesure et de création des états quantiques ont été fabriqués par un adversaire. Jusqu'à présent, les protocoles indépendant-du-dispositif ont été proposés pour la distribution de clés quantiques [AGM06, ABG$^+$07, MY03, BHK05], la génération de nombres aléatoires [Col09, PAM$^+$10], l'estimation d'état [BLM$^+$09], et l'auto-vérification des ordinateurs quantiques [MMMO06].

Il n'est pas clair à priori, s'il est possible de construire des primitives cryptographiques à 2 joueurs dans ce modèle. Cette contrainte nous propose un nouveau défi:

Dans la distribution quantique de clés indépendant-du-dispositif, Alice et Bob coopèrent pour obtenir une clé inconnue d'une tierce personne, Ève. Dans les protocoles à deux joueurs, les joueurs ne se font pas confiance et ne peuvent compter que sur eux-mêmes. Dans le chapitre 7, nous montrons qu'il est possible de réaliser des primitives cryptographiques à deux joueurs dans ce modèle.

Nous présentons un protocole indépendant-du-dispositif pour la mise-en-gage de bit, dans lequel, Alice et Bob peuvent tricher avec une probabilité au plus $\cos^2(\Pi/8) \approx 0,854$. Nous utilisons ensuite ce protocole pour construire un pile-ou-face indépendant-du-dispositf avec une probabilité de tricher d'au plus $0,836$.

Théorème 7 *Il existe un protocole indépendant-du-dispositif pour la mise-en-gage de bit avec une probabilité de tricher de* $0,854$ *et un protocole de pile-ou-face indépendant-du-dispositif avec une probabilité de tricher de* $0,836$.

Il s'agit de la première construction de protocoles indépendant-du-dispositif pour les primitives cryptographiques quantiques à deux joueurs.

1.4.2 Pile-ou-face quantique tolérant aux pertes

Nous considérons maintenant un modèle où les joueurs n'ont pas de mémoire quantique et les dispositifs de mesure ont des pertes. En 2008, Berlin *et al.* ont présenté une pièce de monnaie quantique tolérante aux pertes avec des probabilités de tricher de $0,9$[BBBG08]. Dans ce protocole, les joueurs honnêtes ne réussissent pas toujours à avoir un résultat quand ils effectuent une mesure (la mesure peut parfois échouer) mais quand ils y parviennent, ils ont toujours le résultat correct. Ceci est à distinguer de la tolérance au bruit où un joueur honnête pourrait effectuer une mesure avec un résultat faux sans le savoir. Très récemment, Aharon *et al.* [AMS10] ont créé un pile-ou-face quantique tolérant aux pertes avec une probabilité de tricher de $0,8975$. Dans un contexte un peu différent, Barrett et Massar [BM04] ont montré comment générer aléatoirement une chaîne de bits (une notion plus faible que le pile-ou-face) en présence de bruit.

Le protocole de Berlin *et al.* est le suivant

- Alice envoie un état σ à Bob.
- Bob mesure cet état dans une base B (qui peut dépendre d'un aléa privé de Bob). Si la mesure réussit, ils continuent le protocole. Sinon, ils recommencent.

Dans ce protocole, l'état σ doit être choisi très soigneusement pour qu'un Bob tricheur ne puisse pas utiliser le fait qu'une mesure ratée réinitialise le protocole.

Ceci limite fortement les choix possibles pour σ. Pour résoudre partiellement ce problème, on utilise la méthode suivante :

- Alice choisit $r \in_R \{0,1\}$ et envoie $E_r(\sigma)$ où E_r est une opération quantique de chiffrement qui cache de l'information sur σ.

- Bob mesure dans une base B. Si la mesure réussit, on continue le protocole, sinon on recommence.
- Alice révèle r puis ils continuent comme dans le protocole précédent.

En appliquant cette méthode, en répétant le protocole de Berlin *et al.* deux fois en parallèe, nous montrons que

Théorème 8 *Il existe un protocole quantique de pile-ou-face tolérant aux pertes avec une probabilité de tricher de* $0,859$

Sans cette étape de cryptage supplémentaire, le protocole résultant ne serait pas tolérant aux pertes.

Cette technique qui fait face aux pertes semble très générique. Il serait intéressant de voir si ces techniques peuvent être utilisées dans d'autres modèles pratiques. Trouver un pile-ou-face quantique tolérant au bruit demeure une question ouverte principale.

1.5 Relations entre les preuves sans-connaissance quantiques et la mise-en-gage de bit quantique

Dans la dernière partie de cette thèse, nous allons au-delà de la sécurité inconditionnelle des primitives cryptographiques et étudions les protocoles sans-connaissance quantiques. Nous étudions quelles sont les hypothèses calculatoires qui impliquent la mise-en-gage de bit. Nous allons montrer que l'existence de protocoles quantiques de mise-en-gage de bit est étroitement liée aux protocoles sans-connaissance quantiques et aux classes de preuves interactives.

Pour illustrer ce que sont les protocoles sans-connaissance, prenons un exemple.

Considérons un problème P considéré comme difficile à résoudre. Supposons qu'une personne (le prouveur) veuille révéler à une autre personne (le vérificateur) que la réponse au problème P est OUI, sans donner aucune autre information. En particulier, le vérificateur ne sera pas en mesure de convaincre quelqu'un d'autre que la réponse à ce problème est OUI. Afin de créer ce genre de preuves, le prouveur et le vérificateur doivent interagir. La condition "sans donner d'autres informations" a été formalisée de manière simple et élégante [GMR89] et cette condition de sécurité a été définie à la fois en sécurité calculatoire ainsi qu'en sécurité inconditionnelle. Ces protocoles sont très utiles en cryptographie par exemple pour l'identification sécurisée. La classe des problèmes qui peuvent être résolus avec un protocole sans-connaissance est appelée PZK, SZK si on permet la fuite de très peu d'information, ou ZK si nous supposons que le vérificateur a une puissance de calcul polynomiale.

Ces classes sans-connaissance ont été étendues au cas quantique [Wat02, Kob07, Wat09] où nous permettons aux joueurs d'interagir quantiquement et d'effectuer des opérations quantiques. Les classes correspondantes sont QPZK, QSZK, QZK.

Il y a une relation étroite entre les protocoles sans-connaissance et les protocoles de mise-en-gage de bit. Tout d'abord, nous pouvons construire un protocoles sans-connaissance pour tout problème dans PSPACE si nous avons un protocole de mise-en-gage de bit. D'autre part, nous pouvons construire

des protocoles de mise-en-gage de bit basés sur la difficulté des problèmes de SZK[OW93].

Nous avons d'abord étendu ce résultat au cas quantique et nous avons montré que :

Théorème 9 *SI* QSZK $\not\subseteq$ QMA*, alors il existe un protocole quantique de mise-en-gage de bit avec une sécurité inconditionnelle pour Alice et une sécurité calculatoire pour Bob.*

où QMA est un équivalent quantique de NP (ou plus précisément de MA. La condition QSZK $\not\subseteq$ QMA est considérée comme plausible. Récemment, un oracle pour séparer ces deux classes a été trouvé par Aaronson [Aar11].

Nous nous sommes ensuite intéressés à la mise-en-gage de bit où les joueurs ont aussi l'aide d'un état quantique (potentiellement difficiles à construire). Nous montrons qu'une telle famille de protocoles de mise-en-gage existe sous une hypothèse très faible, à savoir :

Théorème 10 *Si* QIP $\not\subseteq$ QMA*, alors il existe un protocole quantique de mise-en-gage de bit avec aide quantique, avec une sécurité inconditionnelle pour Alice et calculatoire pour Bob.*

Notez que cette hypothèse est très probable vu que QMA $\subseteq$ PP $\subseteq$ PSPACE $=$ QIP et que ces inclusions sont probablement strictes. Dans nos deux théorèmes, on peut choisir pour quel joueur la sécurité est calculatoire.

1.6 Organisation de la thèse

- Dans le chapitre 3 nous présentons les notions de base de l'informatique quantique.
- Dans le chapitre 4, nous étudions le pile-ou-face quantique et montrons comment construire un pile-ou-face optimal *i.e.* un protocole avec une probabilité de tricher d'au plus $\frac{1}{\sqrt{2}} + \varepsilon$ pour tout $\varepsilon > 0$, améliorant le meilleur protocole existant qui avait une probabilité de tricher égale à 3/4. Ce travail a été réalisé avec Iordanis Kerenidis [CK09].
- Dans le chapitre 5, nous étudions les protocoles quantiques de mise-en-gage de bit. Nous établissons d'abord une borne inférieure de $0,739$ pour cette primitive. Nous montrons ensuite comment construire un protocole de mise-en-gage de bit presque optimal, avec une probabilité de tricher d'au plus $0,739 + \varepsilon$ pour tout $\varepsilon > 0$. Nous montrons aussi une borne inférieure pour les protocoles classiques de mise-en-gage où on ajoute la capacité d'effectuer des lancers de pièce parfaits. Il s'agit d'un travail conjoint avec Iordanis Kerenidis [CK11].
- Dans le chapitre 6, nous étudions la transmission inconsciente quantique. Cette étude est la première qui donne des bornes constantes pour cette primitive. Nous établissons d'abord une borne inférieure pour le transfert quantique oublieux de $0,58$. Nous montrons ensuite comment construire un protocole de transmission inconsciente quantique avec une probabilité de tricher de 3/4. Ce travail a été réalisé avec Iordanis Kerenidis et Jamie Sikora [CKS10].

- Dans le chapitre 7, nous étudions ces primitives cryptographiques dans le modèle indépendant-du-dispositif. Nous montrons comment construire un protocole indépendant-du-dispositif de mise-en-gage de bit avec une probabilité de tricher de $0,854$ pour Alice et $3/4$ pour Bob. Nous étendons ensuite cette construction pour construire un pile-ou-face dans ce même modèle avec une probabilité de tricher égale à $0,836$. Ce travail a été réalisé en collaboration avec Jonathan Silman, Nati Aharon, Iordanis Kerenidis, Stefano Pironio et Serge Massar [SCA+11].

- Dans le chapitre 8, nous construisons un pile-ou-face quantique sécurisé contre les pertes avec une probabilité de tricher de $0,859$. Cette construction donne également un protocole quantique de mise-en-gage de bit tolérant aux pertes avec la même probabilité de tricher [Cha10].

- Enfin, au chapitre 9, nous donnons des hypothèses calculatoires reliées aux protocoles sans-connaissance qui permettent de construire des protocoles de mise-en-gage de bit avec une sécurité calculatoire. Il s'agit d'un travail conjoint avec Iordanis Kerenidis et Bill Rosgen [CKR11].

Cette thèse est basée sur les publications suivantes :

[CK09] André Chailloux and Iordanis Kerenidis, *Optimal quantum strong coin flipping.* Foundations of Computer Science (FOCS'09), 0:527–533, 2009.

[CK11] André Chailloux and Iordanis Kerenidis, *Optimal bounds for quantum bit commitment.* Foundations of Computer Science (FOCS'11), 2011.

[CKS10] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. *Lower bounds for Quantum Oblivious Transfer.* IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)

[SCA+11] Jonathan Silman, André Chailloux, Nati Aharon, Iordanis Kerenidis, Stefano Pironio, and Serge Massar. *Fully distrustful quantum bit-commitment and coin flipping.* Physical Review Letters (PRL), 2011.

[Cha10] André Chailloux. *Improved loss-tolerant quantum coin flipping.* AQIS'10

[CKR11] André Chailloux, Iordanis Kerenidis, and Bill Rosgen. *Quantum Commitments from Complexity Assumptions.* International Colloquium on Automata, Languages and Programming (ICALP'11)

J'ai également publié les articles suivants qui ne sont pas présentés dans cette thèse

[CCKV08] André Chailloux, Dragos Florin Ciocan, Iordanis Kerenidis and Salil Vadhan. *Interactive and non-interactive zero knowledge are equivalent in the help model.* Proceedings of the 5th conference on Theory of cryptography (TCC'08)

[CK08] André Chailloux and Iordanis Kerenidis, *Increasing the power of the verifier in Quantum Zero Knowledge.* IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2008)

Certains de ces résultats sur les protocoles sans connaissance apparaissent dans mon mémoire de Mastère:
A study of classical and quantum zero-knowledge protocols using alternative models

Chapter 2

Introduction

2.1 Quantum computing

Quantum mechanics is one of the most important discoveries of the last century in theoretical physics. Thanks to quantum mechanics, we know that at a very small scale, particles behave very differently than what we thought before. At this scale, particles are at several states at the same time and they are modified when observed. Even though these concepts have been developed in the late 1920's, there are still many mysteries related to this theory because of its counterintuitive nature. Still, many experiments have confirmed the quantum nature of the world.

In the mid-80's, the physicist Richard Feynman had a remarkable idea: If we can control some quantum particles, we are able to simulate physical systems in a more efficient way. From his article [Fey82], quantum computing was born. The basic idea is that instead of working on bits that take the value 0 or 1, we work on qubits that are superpositions of bits. A qubit takes the value 0 and 1 with some related coefficients.

There are two main advantages of quantum computing. By manipulating qubits in superposition, we could be able to make some computations in parallel and solve some problems much more quickly than in the classical case. In 1994, Peter Shor discovered that factoring (see Figure 2.1) can be done in polynomial time by a quantum computer [Sho94]. This means that every cryptographic application based on the hardness of factoring (including RSA) can be broken using a quantum computer. This result raised much interest in quantum computing which has now become a very wide and fruitful research topic. Another witness of quantum superiority : Grover showed that one can find an item in database of size n in time $O(\sqrt{n})$ [Gro97] using a quantum computer instead of $O(n)$ for a classical computer. However, such quantum algorithms are still very difficult to implement since it is hard to control many qubits simultaneously.

Another important feature of quantum states is that they lose their quantum behavior when observed. As long as a quantum state is not observed, it is in a superposition of states. However, when it is observed, it chooses probabilistically in which state it is. This means in particular that a quantum state changes when observed. In 1984, Bennett and Brassard [BB84] showed how

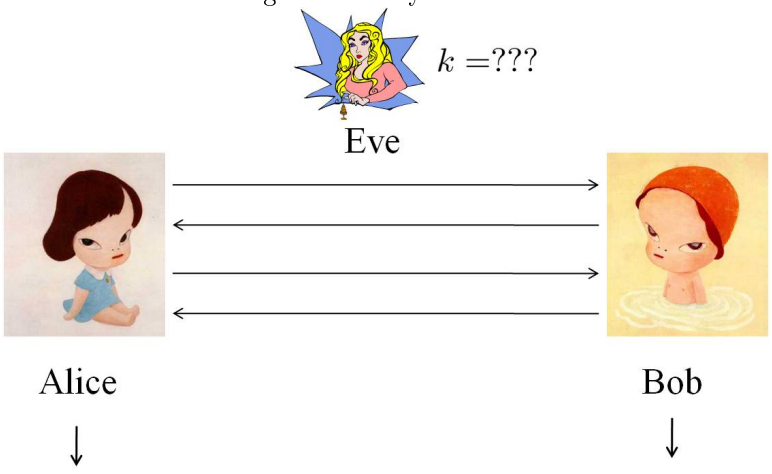
Figure 2.1: Factoring

- Input: any number $n = p \cdot q$ where p, q are prime numbers and $p, q \neq 1$
- Goal: find p and q

For example, if $n = 657713791279$, the goal is to find out that $657713791279 = 660661 \cdot 995539$. Typically, when n has 500 digits (when p, q can have each around 50 digits), the problem is hard for a classical computer but could be easily solved by a quantum computer.

to use this fact to perform quantumly a cryptographic task: Key Distribution (Figure 2.1), which is impossible to perform unconditionally using only classical computers. Since then, Quantum Cryptography has also been developed in many directions. Note also that it is already possible to implement such protocols in practice. The cost and efficiency of quantum cryptography is still worse than its classical counterpart but it becomes more and more a viable solution and several companies sell such quantum devices.

Figure 2.2: Key distribution



Alice and Bob communicate quantumly. At the end, they want to share a common string k. Eve should not be able to gather information about the key k without Alice and Bob noticing.

2.2 Cryptographic primitives

Cryptography is the practice and study of hiding information. Applications of cryptography include ATM cards, electronic commerce or more simply the

possibility of sending an email without being spied on. Cryptography is widely used in everyday life.

If we had to analyze and prove security for each cryptosystem separately, the probability of making errors would be huge so we use some basic building blocks and assemble them to build more complex cryptosystems. It is these building blocks, that we call *cryptographic primitives*, that will be studied in this thesis.

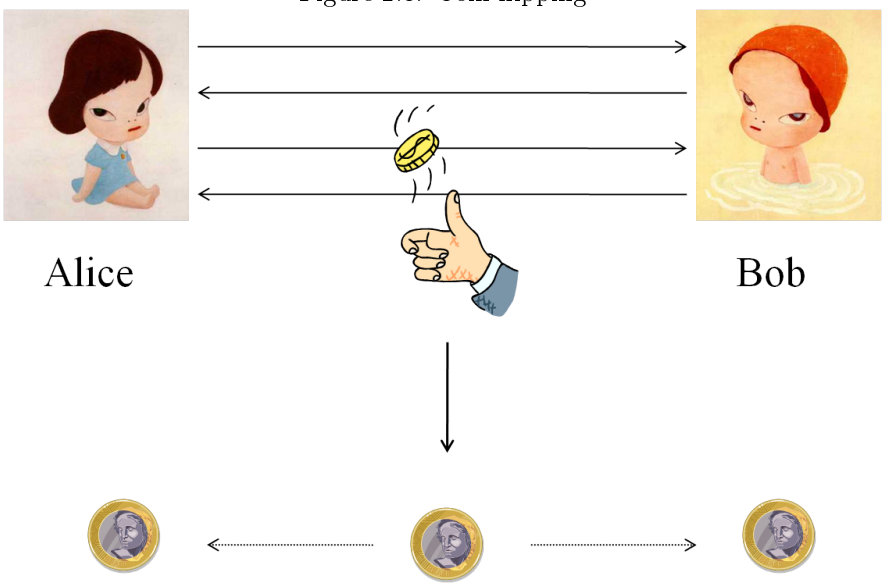
We study here some fundamental cryptographic primitives: *coin flipping*,*bit commitment* and *oblivious transfer*.

Coin flipping is a cryptographic primitive that enables two distrustful and far apart parties, Alice and Bob, to create a random bit that remains unbiased even if one of the players tries to force a specific outcome. It was first proposed by Blum [Blu81] and has since found many applications in two-party secure computation.

A *bit commitment* protocol consists of two phases: in the commit phase, Alice commits to a bit b; in the reveal phase, Alice reveals the bit to Bob. We want to ensure two things: that Bob has no information about b after the commit phase and that Alice cannot change her mind when revealing b.

Oblivious transfer is the strongest primitive since it is a universal primitive for any two-party secure computation [Rab81, EGL82, Cré87] which means that if one can perform perfect Oblivious Transfer, one can perform almost any kind of two party secure computation. We study more precisely 1-out-of-2 random oblivious transfer protocols. In such protocols, Alice outputs two uniformly random bits (x_0, x_1) and Bob outputs x_b for a uniformly random choice of b. The goal of the protocol is to ensure that Bob has no information about $x_{\overline{b}}$ and that Alice has no information about b.

Figure 2.3: Coin flipping



Alice and Bob are far away. They want to flip a coin but do not trust each other.

In the classical setting, all these primitives are widely used to construct cryptosystems, so quantum computing does not seem to be necessary. However, all these classical protocols rely on some computational assumption. For example, it is possible to perform (almost) perfect coin flipping under the assumption that factoring is hard. All current classical cryptographic primitives rely on such hardness assumptions. We say that such primitives are *computationally secure*.

A stronger notion of security is *information theoretic* security. In this setting, the primitives must be secure even against an all powerful cheating player - typically a player who can easily factor and easily perform any kind of operation. In the classical setting, we know that it is impossible to achieve information theoretic security for most of these cryptographic primitives. Even worse, when considering all powerful cheating players, we have the following statement

In any classical coin flipping, bit commitment or oblivious transfer protocol, there is a party which can cheat with probability 1 *in the information theoretic setting (i.e. the cheating player is computationally unbounded)*

This means that such primitives are impossible to perform in the classical model of computation.

2.3 Physical limitations of quantum cryptographic primitives

Quantum information has given us the opportunity to revisit information theoretic security in cryptography. The first breakthrough result was the quantum key distribution protocol of Bennett and Brassard [BB84]. Thenceforth, a long series of work has focused on which other cryptographic primitives are possible with the help of quantum information. Unfortunately, the subsequent results were not positive. Mayers and Lo, Chau proved the impossibility of secure quantum bit commitment and oblivious transfer and consequently of any type of two-party secure computation [May97, LC97, DKSW07].

These impossibility results rule out the ability to build perfect cryptographic primitives. However, it could be possible to build some quantum cryptographic primitives which are almost perfect. Aharanov *et al.* [ATVY00] first showed how to construct imperfect quantum bit commitment with cheating probabilities smaller than 0.9143. The best protocol was due to Ambainis who constructed a quantum bit commitment scheme (and a quantum coin flipping protocol) where no player can cheat with probability greater than 3/4 [Amb01].

There is a quantum coin flipping protocol and a quantum bit commitment scheme, where each player can cheat with probability at most 3/4.

On the other hand, Kitaev showed that it is not possible to build quantum coin flipping protocols which have low cheating probability in the information theoretic setting [Kit03]:

In any quantum coin flipping or quantum bit commitment scheme, there is a player who can cheat with probability at least $\frac{1}{\sqrt{2}}$.

The way to interpret this is that the laws of quantum physics allow us theoretically to construct coin flipping protocols with cheating probability 3/4; but no physically realizable coin flipping protocol with cheating probability less than $\frac{1}{\sqrt{2}}$ exists.

There is also another notion of coin flipping which has been studied: Quantum Weak Coin Flipping. In this case, we want to make sure that Alice cannot force the heads outcome and that Bob cannot force the tails outcome. However, unlike regular coin flipping, Alice can force the tails outcome with probability 1 and Alice can force the heads outcome with probability 1. After a series of works [Moc04, Moc05, Moc07], Mochon showed how to build a quantum Weak Coin Flipping protocol which is almost perfectly secure. As opposed to this weak notion of coin flipping, we will refer to the standard coin flipping as *strong coin flipping*. Notice that even for this weaker definition, it is impossible to exhibit such a classical protocol.

We greatly improve these physical bounds for quantum cryptographic primitives. In Chapter 4, we study quantum coin flipping. We show here how to construct a quantum coin flipping protocol with cheating probability arbitrarily close to $\frac{1}{\sqrt{2}}$. From Kitaev's lower bound, we know that our protocols are arbitrarily close to optimal. More precisely, we show the following

Theorem 1 *For any $\varepsilon > 0$, there exists a strong coin flipping protocol with cheating probability $\frac{1}{\sqrt{2}} + \varepsilon$.*

To show this, we actually use Mochon's construction of optimal quantum weak coin flipping. We build a classical protocol where we use weak coin flipping as a subroutine. This means that the ability to perform strong coin flipping with cheating probability $\frac{1}{\sqrt{2}}$ comes from the ability to perform optimal weak coin flipping. Equivalently, if we could build a perfect classical weak coin then our construction would give a classical strong coin flipping with cheating probability $\frac{1}{\sqrt{2}}$.

We then investigate the physical bounds for quantum bit commitment. Before our work, the bounds for quantum coin flipping and quantum bit commitment were the same. It was not clear whether these two primitives had the same optimal bound or not. In Chapter 4, we show that this is not the case. We first show an improved lower bound for quantum bit commitment.

Theorem 2 *In any quantum bit commitment protocol, at least one of the players can cheat with probability at least* 0.739.

Then, we provide a matching upper bound. We describe a quantum bit commitment protocol that achieves a cheating probability arbitrarily close to 0.739. Our protocol uses a weak coin flipping protocol with cheating probability $1/2+\epsilon$ as a subroutine and achieves a cheating probability for the bit commitment of $0.739 + O(\epsilon)$.

Theorem 3 *For any $\varepsilon > 0$, there exists a quantum bit commitment protocol that achieves cheating probabilities less than* $0.739 + \varepsilon$.

This protocol also uses Mochon's quantum weak coin flipping. However this protocol is in fact quantum even beyond the weak coin flip subroutine. This is in fact necessary. We show that any classical bit commitment protocol with access

to a perfect weak coin (or even strong coin) cannot achieve cheating probability less than 3/4.

Theorem 4 *Any classical bit commitment protocol with access to perfect weak (or strong) coin flipping cannot achieve cheating probabilities less than* 3/4.

Unlike the case of quantum strong coin flipping that is derived classically when one has access to a weak coin flipping protocol, the optimal quantum bit commitment takes advantage of quantum effects beyond the weak coin flipping subroutine.

In Chapter 5, we extend these results to Oblivious Transfer. We present the first bounds for quantum oblivious transfer. Unlike quantum coin flipping and bit commitment, we were not able to find an optimal value for quantum oblivious transfer. We first show an upper lower bound for quantum oblivious transfer

Theorem 5 *In any quantum oblivious transfer protocol, at least one of the players can cheat with probability* 0.58

To prove this Theorem, we reduce any Oblivious transfer protocol to a bit commitment protocol. We then use the lower bounds on quantum bit commitment to conclude. Notice however, that the resulting bit commitment protocol does not have the same cheating probabilities as the original oblivious transfer protocol, this is why the lower bound for quantum oblivious transfer is worse than the lower bound for quantum bit commitment.

We then construct a protocol with cheating probability 3/4.

Theorem 6 *There exists a quantum oblivious transfer protocol that achieves cheating probabilities of* 3/4

The following tables present old bounds and new bounds obtained in this thesis for quantum cryptographic primitives, for any $\varepsilon > 0$.

Old bounds for quantum cryptographic primitives

	lower bound	upper bound
Weak Coin Flipping	$1/2$	$1/2 + \varepsilon$
Strong Coin Flipping	$\frac{1}{\sqrt{2}}$	$3/4$
Bit Commitment	$\frac{1}{\sqrt{2}}$	$3/4$
Oblivious transfer	*	*

* Bounds for quantum oblivious transfer have been studied in [SSS09]. The bounds obtained were in terms of entropy for a stronger notion of oblivious transfer. These bounds are incomparable with the types of bounds we obtain here

New bounds for quantum cryptographic primitives

	lower bound	upper bound
Weak Coin Flipping	$1/2$	$1/2 + \varepsilon$
Strong Coin Flipping	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}} + \varepsilon$
Bit Commitment	0.739	$0.739 + \varepsilon$
Oblivious Transfer	0.58	$3/4$

2.4 Practical models for two party quantum cryptographic primitives

In the first part, we studied the possibilities and the limits of information theoretic quantum cryptography. We now investigate the possibility of practically implementing such primitives. This has extensively been done for Quantum Key Distribution. It has also been done for two party quantum cryptographic primitives but not in the information theoretic setting. Our goal is to see how possible it is to implement such primitives in the information theoretic setting. Of course, our results will be weaker than the ones for Quantum Key Distribution since we are limited by the lower bounds described in the previous part, hence our protocols will always have constant cheating probabilities.

2.4.1 The device independent model

A quantum protocol is said to be device-independent if the reliability of its implementation can be guaranteed without making any assumptions regarding the internal workings of the underlying apparatus. The key idea is that the certification of a sufficient amount of non-locality ensures that the underlying systems are quantum and entangled. By dispensing with the (mathematically convenient but physically untestable) notion of a Hilbert space of a fixed dimension, the device independent approach does away with many cheating mechanisms and modes of failure, such as, for example, those exploited in [XQL10, LWW$^+$10]. In fact, a device independent protocol, in principle, remains secure even if the devices were fabricated by an adversary. So far, device independent protocols have been proposed for quantum key distribution [AGM06, ABG$^+$07, MY03, BHK05], random number generation [Col09, PAM$^+$10], state estimation [BLM$^+$09], and the self-testing of quantum computers [MMMO06].

It is not a priori clear, whether the scope of the device independent approach can be extended to cover cryptographic problems with distrustful parties. In particular, this setting presents us with a novel challenge: Whereas in device independent quantum key-distribution Alice and Bob will cooperate to estimate the amount of nonlocality present, for protocols in the distrustful cryptography model, honest parties can rely only on themselves. In Chapter 7, we show that protocols in this model are indeed amenable to a device independent formulation. As our aim is to provide a proof of concept, we concentrate on one of the simplest, yet most fundamental, primitives in this model, bit commitment. We present a device independent bit commitment protocol, wherein after the commit phase Alice cannot control the value of the bit she wishes to reveal with probability greater than $\cos^2\left(\frac{\pi}{8}\right) \approx 0.854$ and Bob cannot learn its value prior to the reveal phase with probability greater than $\frac{3}{4}$. We then use this protocol to construct a device independent coin flipping protocol with cheating probability smaller than approximately 0.836.

Theorem 7 *There exists a device-independent quantum bit commitment protocol with cheating probability* 0.854 *and a quantum coin flipping protocol with cheating probability* 0.836.

This is the first construction of device independent protocols for two party quantum cryptographic primitives.

2.4.2 Quantum loss-tolerant coin flipping

We are now interested in the loss-tolerant model where honest players do not have any quantum memory and the measurement devices have some losses. In 2008, Berlin *et al.* presented a loss-tolerant quantum coin flipping with cheating probabilities 0.9 [BBBG08]. In this protocol, honest players do not always succeed when they perform a measurement (the measurement sometimes abort) but when they do succeed, they always output the correct value. This is in contrast with noise tolerance where an honest player could perform a measure with a wrong outcome without knowing it. Very recently, Aharon *et al.* [AMS10] created a loss-tolerant quantum coin flipping protocol with cheating probability 0.3975. In another flavor, Barrett and Massar [BM04] showed how to do bit-string generation (a weaker notion of coin flipping) in the presence of noise.

We continue Berlin *et al.* 's work work and create a loss-tolerant quantum coin flipping protocols where the players can chat with probability at most 0.359. As in Berlin *et al.* 's protocol, we ask Alice and Bob to send several copies of single qubit states. Moreover, we do not require honest players to have any quantum memories and consider cheating players as being all powerful.

Berlin *et al.* 's protocol is of the following form.

- Alice sends a state σ to Bob.
- Bob measures this state in some basis B (possibly dependent on some of his private coins). If Bob successfully measures then they continue the protocol. Otherwise, they start again

In this protocol, the state σ is chosen very carefully such that a cheating Bob cannot take advantage of the fact, that he can reset the protocol. This strongly limits the good choices for σ. To partially overcome this problem, we use the following high-level scheme

- Alice picks $r \in_R \{0,1\}$ and sends $E_r(\sigma)$ where E_r is some quantum operation that hides some information about σ
- Bob measures in some basis B. If Bob successfully measures then they continue the protocol. Otherwise, they start again
- Alice reveals r and then they continue the protocol

While doing this, one must be careful that an honest Bob will still be able to exploit the measurement of the encrypted state and that Alice cannot use this to cheat.

Applying this scheme on a two-fold parallel repetition of Berlin *etal*'s protocol, we show the following

Theorem 8 *There is a loss-tolerant quantum coin flipping protocol where any cheating player can cheat with probability at most* 0.859*.*

Notice that without this extra encryption step, the resulting scheme would not be loss-tolerant but the bias would remain the same.

This technique to deal with losses seems very generic. It would be interesting to see whether such techniques can be used in other practical models. Moreover, finding a noise-tolerant quantum coin flipping with information theoretic security and small cheating probability remains an interesting open question.

2.5 Relationship between quantum zero-knowledge proofs and quantum bit commitment

In the last part of this thesis, we go a little beyond the scope of information theoretic quantum cryptography and study quantum computational bit commitment schemes. We study complexity assumptions that imply such commitment schemes. We will show that the existence of quantum computationally secure bit commitments is closely related to quantum zero-knowledge classes and quantum interactive proofs.

To illustrate what zero-knowledge protocols are, let us consider an example. Consider a problem P believed to be hard to solve. Suppose that one person (the Prover) can prove to another person (the Verifier) that the answer to the problem is YES without giving any other information. In particular, the Verifier will not be able to convince someone else that the answer to this problem is YES. In order to create this kind of proofs, the Prover and the Verifier must interact with each other. The condition "Without giving any other information" has been formalized in a simple and elegant way by [GMR89] and this security condition has been defined in the computational setting as well as the information-theoretical setting. Such protocols are very useful in cryptography for example in secure identification. The class of problems that can be solved with a zero-knowledge protocol is called PZK, SZK if one allows to leak a (very) small amount of information, or ZK if we assume that the verifier has polynomial computational power.

These zero-knowledge classes have been extended to the quantum case [Wat02, Kob07, Wat09] where we allow the players to interact quantumly and to perform quantum operations. The resulting classes are QPZK, QSZK, QZK.

There is a tight relationship between bit commitment schemes and zero-knowledge proofs. First of all, we can construct a zero-knowledge for any problem in PSPACE if we have a bit commitment scheme [BGG$^+$90]. On the other hand, we can construct bit commitment schemes based on the hardness of SZK problems [OW93].

We first extend this result to the quantum case and show the following:

Theorem 9 *If* QSZK $\not\subseteq$ QMA*, then there exists a quantum commitment scheme which is information theoretically secure for the Sender and computationally secure for the receiver.*

QMA is the quantum equivalent of NP. Notice that this condition is believed to be true. Recently, an oracle separating these two classes was found by Aaronson [Aar11]. Notice also that the commitments we construct are non-uniform, which means that the players receive some classical advice in order to perform this commitment.

We are then interested in commitments where the players have as advice a quantum state (potentially hard to construct). We show that such commitment exists under a very weak assumption, namely

Theorem 10 *If* QIP $\not\subseteq$ QMA*, then there exists quantum commitment scheme with quantum advice which is information theoretically secure for the Sender and computationally secure for the receiver.*

This is highly plausible since $\mathsf{QMA} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE} = \mathsf{QIP}$ and these containments are believed to be strict. Note that in both our Theorems, we can exchange the player for which we have computational security.

2.6 Organization

- In Chapter 3, we present the basic notions of quantum mechanics.
- In Chapter 4, we study quantum coin flipping and show how to construct an optimal quantum strong coin flipping, *i.e.* a protocol with cheating probability at most $\frac{1}{\sqrt{2}} + \varepsilon$ for any $\varepsilon > 0$, improving the previously best known protocol which achieved a cheating probability of 3/4. This is joint work with Iordanis Kerenidis [CK09].
- In Chapter 5, we study quantum bit commitment. We first show a lower bound for quantum bit commitment of 0.739. We then show how to construct an optimal quantum strong coin flipping, *i.e.* a protocol with cheating probability at most $0.739 + \varepsilon$ for any $\varepsilon > 0$. We also show a lower bound on classical bit commitment protocols where the ability to perform coin flipping is given for free. This is joint work with Iordanis Kerenidis [CK11].
- In Chapter 6, we study quantum oblivious transfer. This is the first study that gives some constant bounds for quantum oblivious transfer. We first show a lower bound for quantum oblivious transfer of 0.58. We then show how to construct a quantum oblivious transfer protocol with cheating probability 3/4. This is joint work with Iordanis Kerenidis and Jamie Sikora [CKS10].
- In Chapter 7, we study quantum coin flipping and quantum bit commitment in the device independent model. We show how to construct a device independent bit commitment scheme with cheating probability 0.854 for Alice and 3/4 for Bob. We then extend this construction to build a device independent quantum coin flipping with cheating probabilities 0.836. This is joint work with Jonathan Silman, Nati Aharon, Iordanis Kerenidis, Stefano Pironio and Serge Massar [SCA+11].
- In Chapter 8, we build a quantum coin flipping protocol secure against losses with cheating probabilities 0.859. This construction also gives a quantum bit commitment scheme secure against losses with the same cheating probabilities [Cha10].
- Finally, in Chapter 9, we show under which assumptions related to quantum zero-knowledge protocols, it is possible to create quantum bit commitment schemes which are computationally secure. This is joint work with Iordanis Kerenidis and Bill Rosgen [CKR11].

This thesis is based on the following publications:

[CK09] André Chailloux and Iordanis Kerenidis, *Optimal quantum strong coin flipping.* Foundations of Computer Science (FOCS'09), 0:527–533, 2009.

[CK11] André Chailloux and Iordanis Kerenidis, *Optimal bounds for quantum bit commitment.* Foundations of Computer Science (FOCS'11), 2011.

[CKS10] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. *Lower bounds for Quantum Oblivious Transfer.* IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)

[SCA+11] Jonathan Silman, André Chailloux, Nati Aharon, Iordanis Kerenidis, Stefano Pironio, and Serge Massar. *Fully distrustful quantum bit-commitment and coin flipping.* Physical Review Letters (PRL), 2011 (To Appear).

[Cha10] André Chailloux. *Improved loss-tolerant quantum coin flipping.* AQIS'10

[CKR11] André Chailloux, Iordanis Kerenidis, and Bill Rosgen. *Quantum Commitments from Complexity Assumptions.* International Colloquium on Automata, Languages and Programming (ICALP'11)

I also published some articles which are not contained in the present manuscrpit:

[CCKV08] André Chailloux, Dragos Florin Ciocan, Iordanis Kerenidis and Salil Vadhan. *Interactive and non-interactive zero knowledge are equivalent in the help model.* Proceedings of the 5th conference on Theory of cryptography (TCC'08)

[CK08] André Chailloux and Iordanis Kerenidis, *Increasing the power of the verifier in Quantum Zero Knowledge.* IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2008)

Some preliminary results contained in these articles can be found in my master's thesis:
A study of classical and quantum zero-knowledge protocols using alternative models

Chapter 3

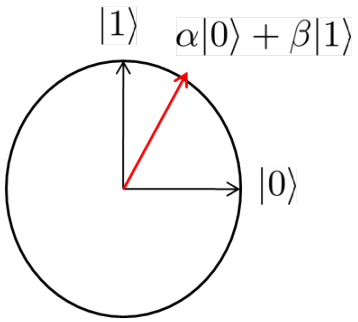
Quantum Preliminaries

In this Chapter, we present the standard model of quantum computing.

3.1 Pure states

A qubit is the quantum equivalent of a bit. Unlike classical bits, quantum bits can be in a superposition of states. We call such quantum states *pure states*. A 1-qubit pure state $|q\rangle$ is a superposition of 0 and 1 with certain amplitudes. We will denote it $|q\rangle = a|0\rangle + b|1\rangle$ with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. $|q\rangle$ is fully determined by these 2 amplitudes a and b and can be represented by the complex vector $\binom{a}{b}$ of norm 1. Let Q_1 the Hilbert space of 1-qubit pure states. $Q_1 = \{a, b \in \mathbb{C} \ : \ |a|^2 + |b|^2 = 1\}$. If we restrict ourselves to $a, b \in \mathbb{R}$, we can represent a qubit on the unit circle

Figure 3.1: Quantum bit on the unit circle



A N-qubit pure state $|q\rangle$ is defined similarly as an element of a Hilbert space. Instead of being the superposition of 2 possible outcomes 0 or 1, it is the superposition of 2^N possible outcomes in $\{0,1\}^N$. We have

$$|q\rangle = \sum_{i=0}^{2^N-1} a_i|i\rangle = a_0|00...0\rangle + a_1|00..01\rangle + \cdots + a_{2^N-1}|11...1\rangle = \begin{pmatrix} a_0 \\ \vdots \\ a_{2^N-1} \end{pmatrix}$$

Where the a_i's are in $\mathbb{C}$ and $\sum_i |a_i|^2 = 1$. We note Q_N the space of N-qubit states.

Dirac's notation : If we note $|q\rangle = a|0\rangle + b|1\rangle$, we write the equality $|q\rangle = a\binom{1}{0} + b\binom{0}{1}$. The $|\cdot\rangle$ notation is for column vectors. We also note $\langle q|$ the line vector ${}^t|\overline{q}\rangle$. This notation is very useful. In particular, if $|q\rangle = \sum_i a_i|i\rangle$ and $|q'\rangle = \sum_i a'_i|i\rangle$, we have $\langle q| \cdot |q'\rangle = \sum_i \overline{a}_i a'_i = \langle q|q'\rangle$ which is the inner-product of q and q'. The outer product $|q\rangle\langle q'|$ will also be useful.

3.2 Operations on quantum bits

There are two operations that can be performed a quantum states: *Unitary operations* and *Measurements*. For a Hilbert space $\mathcal{H}$, we define as $\mathbf{L}(\mathcal{H})$ the set of linear operators on $\mathcal{H}$.

Unitary operations Quantum unitary operations done on quantum pure states are elements of $\mathbf{L}(\mathcal{H})$ which preserve the set of pure states. They are described by matrices of size $2^N \times 2^N$ (for an operation acting on an N-qubit state). Such a unitary M is invertible. Let $M^\dagger$ such that $MM^\dagger = M^\dagger M = \mathcal{I}d$. When applying an operation M to a pure state $|q\rangle$, the result is $M \cdot |q\rangle$ which is a standard multiplication of a matrix and a vector.

Note that when a unitary acts on an N-qubit state, it acts on the superposition of up to 2^N states simultaneously. Quantum operations can be simulated by classical computers but it takes exponential time. This is one of the main reasons why quantum computers are more powerful than classical computers.

Measurements The qubits we have described are not disturbed. The only way to extract information from a qubit is to make a measurement. For example, if we measure a qubit $q = a|0\rangle + b|1\rangle$, we will get 0 with probability $|a|^2$ and 1 with probability $|b|^2$. Note that after the measurement, if for example we measure $|0\rangle$, the qubit now behaves like the qubit $|0\rangle$ and "forgets" his previous state. The measurement works in a similar way when looking at N-qubit states. Similarly, we can measure in any basis $B = (b_1, \ldots, b_{2^N})$. When measuring $|q\rangle$ in basis B, the probability of obtaining b_i is $|\langle b_i|q\rangle|^2$.

Note that you can also do partial measurements. Let $|q\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$. Suppose you measure the first qubit of $|q\rangle$. You'll measure "0" with probability $|a^2| + |b^2|$. If you measure 0 then the second qubit will be in the following state : $\frac{a}{\sqrt{|a|^2+|b|^2}}|0\rangle + \frac{b}{\sqrt{|a|^2+|b|^2}}|1\rangle$. We ignored the parts that started with 1 and renormalized to have total norm one. Similar reasoning can be used when a "1" is measured.

For a quantum state, the most general type of measurement is a *Positive Operator Valued Measure* (or POVM). A POVM consists of n elements $\{E_1, \ldots, E_n\}$ which are positive matrices such that $\sum_i E_i = \mathbb{I}$. When performing such a $POVM$ on a state $|\psi\rangle$, you get outcome i with probability $\langle\psi|E_i|\psi\rangle$.

3.3 Mixed states

Very often, it will be useful to consider probabilistic quantum states. We will call such states *mixed states*. The set of mixed states on a Hilbert space $\mathcal{H}$ is $\mathbf{D}(\mathcal{H})$

A mixed state is of the form $\rho = \begin{cases} wp.\ p_1 \to |e_1\rangle \\ \quad \vdots \quad \vdots \\ wp.\ p_k \to |e_k\rangle \end{cases}$ with $\sum_i p_i = 1$.

which means that with probability p_i, the state behaves like $|e_i\rangle$ where the $|e_i\rangle$'s are pure states. Each mixed state is represented by a density matrix of size $2^N \times 2^N$ of the from

$$\rho = \sum_{i=1}^{k} p_i |e_i\rangle\langle e_i|$$

Note from Dirac's notation that $|e_i\rangle\langle e_i|$ is a matrix of size $2^N \times 2^N$ when the $|e_i\rangle$'s are N qubit-states and the sum is a usual sum of matrices. Density matrices are symmetric and have trace 1. A mixed state $\rho \in \mathbf{D}(\mathcal{H})$ is an element in $\mathbf{L}(\mathcal{H})$ satisfying $tr(\rho) = 1$ and ρ positive.

When applying an operation M to a mixed state ρ, the result is $\rho' = M\rho M^\dagger$. If we measure a mixed state ρ in a basis $B = (b_1, \ldots, b_n)$, the probability of getting b_i is $\langle b_i|\rho|b_i\rangle$. When applying a $POVM$ $\{E_1, \ldots, E_n\}$ to ρ, the outcome is i with probability $p(i) = \mathrm{tr}(E_i\rho)$.

This means that any mixed state is characterized exactly by its density matrix. In particular, if 2 mixed states have the same density matrix then they are indistinguishable in an information theoretical sense. For example, let's define $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and consider the 2 following mixed states

$$\rho_1 = \begin{cases} wp.\ 1/2 \to |0\rangle \\ wp.\ 1/2 \to |1\rangle \end{cases} \quad \text{and} \quad \rho_2 = \begin{cases} wp.\ 1/2 \to |+\rangle \\ wp.\ 1/2 \to |-\rangle \end{cases}$$

If we calculate these density matrices, we have :

$$\rho_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

$$\rho_2 = \frac{1}{2}\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

It means that even though these 2 states are not defined the same way, we say that they are equal. When the density matrix of a state is of the form $\frac{1}{2^n}$ times the identity, we say that this state is the totally mixed state. This state is noted $\mathbb{I}$ or $\mathbb{I}_n$ if we want to specify the number of qubits of this state. In our example, $\rho_1 = \rho_2 = \mathbb{I}_1$.

3.4 On N-qubit states

Tensor products Suppose we have 2 qubits $q_1 = a_1|0\rangle + b_1|1\rangle$ and $q_2 = a_2|0\rangle + b_2|1\rangle$. Consider the 2 qubit state consisting of $|q_1\rangle$ and $|q_2\rangle$. We note that this state $|q\rangle = |q_1\rangle \otimes |q_2\rangle$ and $q = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$. This is called a tensor product.

Entangled states We cannot obtain all the possible N-qubit states by doing only tensor products. Consider for example the 2-qubit state $|q\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We can see that we cannot create this state from the tensor of any 2 states. It means that when we look at each part separately, we do not get pure states. Instead, we get a mixed state. In our example, we have the totally mixed state for each part : $\begin{cases} wp.\ 1/2 : |0\rangle \\ wp.\ 1/2 : |1\rangle \end{cases}$ We say that these 2 halves are entangled.

Entanglement can be used in protocols. Suppose that Alice and Bob each have 1 half of the state $|00\rangle + |11\rangle$. If Alice measures (in the $|0\rangle, |1\rangle$ basis), she will get $|0\rangle$ or $|1\rangle$ with half probability. The same holds for Bob but they both know that they will get the same result. Protocols that allow Alice and Bob to coordinate their actions can be done just by using entangled states.

Tracing out qubits As we have seen, we obtain mixed states by ignoring some parts of a given state. We say that we trace out these ignored qubits. For example, let $|q\rangle$ a pure state that has qubits in a space $A \times B$. If we want to consider the mixed state q_A consisting only of the qubits in A, we write $q_A = \mathrm{Tr}_B(|q\rangle\langle q|)$ (the B part is traced out). Similarly, $q_B = \mathrm{Tr}_A(|q\rangle\langle q|)$.

3.5 Norms

In order to define the statistical distance between quantum states, we use a generalization of the ℓ_1 norm to linear operators. This is the *trace norm* which gives the sum of the singular values of an operator. More formally, the trace norm may be expressed as

$$\| X \|_{\mathrm{tr}} = \sqrt{X^\dagger X} = \max_U |\mathrm{tr}\, XU| , \tag{3.1}$$

where the maximization is taken over all unitaries of the appropriate size.

The *diamond norm* is a generalization of the trace norm to quantum channels that preserves the distinguishability characterization. A quantum channel corresponds to any quantum operation, where can perform unitaries, and trace out some qubits. Given one of two quantum channels Q_0, Q_1 each with equal probability, then the optimal procedure to determine the identity of the channel with only one use succeeds with probability $1/2 + \| Q_0 - Q_1 \|_\diamond / 4$. The definition of the diamond norm is more complicated than the trace norm, however, as the optimal distinguishing procedure may make use of an auxiliary space, sending only a portion of some entangled state through the channel. It is known, however, that the dimension of this auxiliary space does not need to exceed the dimension of the input space [Kit97, Smi83]. The diamond norm, for a linear map from $Q\colon \mathbf{L}(\mathcal{H}) \to \mathbf{L}(\mathcal{K})$ with an auxiliary space $\mathcal{F}$ with $\dim \mathcal{F} = \dim \mathcal{H}$ can be defined as

$$\| Q \|_\diamond = \max_{X \in \mathbf{L}(\mathcal{H} \otimes \mathcal{F})} \frac{\| (Q \otimes I_{\mathcal{F}})(X) \|_{\mathrm{tr}}}{\| X \|_{\mathrm{tr}}}.$$

Closely related to the diamond norm is a known studied in operator theory known as the completely bounded norm. An upper bound on this norm can be found in [Pau02]. Since the diamond norm is dual to this norm, this bound may also be applied also to the diamond norm. See [JKP09] for a discussion of

this bound and the relationship between the diamond and completely bounded norms.

One inconvenient property of the diamond norm is that for some maps the maximum in the definition may not be achieved on a quantum state. Fortunately, in the case of the difference of two completely positive maps it is known that this maximum is achieved by a pure state.

Lemma 1 ([RW05]) *Let $\Phi_0, \Phi_1 \colon \mathbf{L}(\mathcal{H}) \to \mathbf{L}(\mathcal{K})$ be completely positive linear maps and let $\Phi = \Phi_0 - \Phi_1$. Then, there exists a Hilbert space $\mathcal{F}$ and a unit vector $|\phi^*\rangle \in \mathcal{F} \otimes \mathcal{H}$ such that*

$$\| \Phi \|_\diamond = \| (I_\mathcal{F} \otimes \Phi)(|\phi^*\rangle\langle\phi^*|) \|_{\mathrm{tr}}.$$

3.6 How close are two quantum states ?

We start by stating a few properties of the trace distance Δ and fidelity F between two quantum states. These two notions characterize how close are two quantum states.

Trace distance between two quantum states

Definition 1 *For any two quantum states ρ, σ, the trace distance Δ between them is given by $\Delta(\rho,\sigma) = \Delta(\sigma,\rho) = \frac{1}{2}\| \rho - \sigma \|_{\mathrm{tr}}$*

Proposition 1 *For any two states ρ, σ, and a POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho E_i)$ and $q_i = tr(\sigma E_i)$, we have $\Delta(\rho,\sigma) \geq \frac{1}{2}\sum_i |p_i - q_i|$. There is a POVM (even a projective measurement) for which this inequality is an equality.*

Proposition 2 *[Hel67] Suppose Alice has a bit $c \in_R \{0,1\}$ unknown to Bob. Alice sends a quantum state ρ_c to Bob. We have*

$$\Pr[\textit{Bob guesses } c] \leq \frac{1}{2} + \frac{\Delta(\rho_0,\rho_1)}{2}$$

There is a strategy for Bob that achieves the value $\frac{1}{2} + \frac{\Delta(\rho_0,\rho_1)}{2}$.

Proposition 3 *For any two states ρ, σ such that $\rho = \sum_i p_i |i\rangle\langle i|$ and $\sigma = \sum_i q_i |i\rangle\langle i|$, we have*

$$\begin{aligned}\Delta(\rho,\sigma) &= \sum_i \frac{1}{2}|p_i - q_i| = \sum_{i:p_i \geq q_i} (p_i - q_i) \\ &= 1 - \sum_i \min\{p_i, q_i\} = \sum_i \max\{p_i, q_i\} - 1\end{aligned}$$

Proof: Since $\sum_i p_i = \sum_i q_i = 1$, we have $\sum_{i:p_i \geq q_i}(p_i - q_i) = \sum_{i:p_i < q_i}(q_i - p_i)$ and $\sum_i \max\{p_i,q_i\} + \min\{p_i,q_i\} = 2$ hence

$$\Delta(\rho,\sigma) = \sum_i \frac{1}{2}|p_i - q_i| = \frac{1}{2}\left(\sum_{i:p_i \geq q_i}(p_i - q_i) + \sum_{i:p_i < q_i}(q_i - p_i)\right) = \sum_{i:p_i \geq q_i}(p_i - q_i)$$

$$\begin{aligned}\Delta(\rho,\sigma) &= \sum_i \frac{1}{2}|p_i - q_i| = \frac{1}{2}\sum_i (\max\{p_i,q_i\} - \min\{p_i,q_i\}) \\ &= 1 - \sum_i \min\{p_i,q_i\} = \sum_i \max\{p_i,q_i\} - 1\end{aligned}$$

■

Proposition 4 *[NC00] For any two states ρ, σ such that $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ and $\sigma = \sum_i q_i |\phi_i\rangle\langle\phi_i|$, we have*

$$\Delta(\rho, \sigma) \leq \frac{1}{2} \sum_i |p_i - q_i|$$

Fidelity of quantum states

Definition 2 *For any two states ρ, σ, the fidelity F between them is given by $F(\rho, \sigma) = F(\sigma, \rho) = tr(\sqrt{\rho^{\frac{1}{2}} \sigma \rho^{\frac{1}{2}}})$*

Proposition 5 *For any two states ρ, σ, and a POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho E_i)$ and $q_i = tr(\sigma E_i)$, we have $F(\rho, \sigma) \leq \sum_i \sqrt{p_i q_i}$. There is a POVM for which this inequality is an equality.*

Definition 3 *We say that a pure state $|\psi\rangle$ in $\mathcal{A} \otimes \mathcal{B}$ is a purification of some state ρ in $\mathcal{B}$ if $\mathrm{Tr}_{\mathcal{A}}(|\psi\rangle\langle\psi|) = \rho$*

Proposition 6 (Uhlmann's theorem) *For any two quantum states ρ, σ, there exist a purification $|\phi\rangle$ of ρ and a purification $|\psi\rangle$ of σ such that $|\langle\phi|\psi\rangle| = F(\rho, \sigma)$*

Proposition 7 *For any two quantum states ρ, σ and a completely positive trace preserving operation Q, we have $F(\rho, \sigma) \leq F(Q(\rho), Q(\sigma))$.*

Proposition 8 ([SR01, NS03]) *For any two quantum states ρ, σ*

$$\max_{\xi} \left(F^2(\rho, \xi)^2 + F^2(\xi, \sigma) \right) = 1 + \mathrm{F}(\rho, \sigma).$$

Proposition 9 ([FG99]) *For any quantum states ρ, σ, we have*

$$1 - F(\rho, \sigma) \leq \Delta(\rho, \sigma) \leq \sqrt{1 - F^2(\rho, \sigma)}$$

Chapter 4

Optimal Quantum strong coin flipping

Coin flipping is a cryptographic primitive that enables two distrustful and far apart parties, Alice and Bob, to create a random bit that remains unbiased even if one of the players tries to force a specific outcome. It was first proposed by Blum [Blu81] and has since found many applications in two-party secure computation.

The goal here is to present a quantum strong coin flipping protocol where any player can bias the coin with probability at most $\frac{1}{\sqrt{2}} + \varepsilon$ for any $\varepsilon > 0$. This protocol is based on a quantum weak coin flipping protocol by Mochon where any cheating player can cheat with probability at most $\frac{1}{2} + \varepsilon$ for any $\varepsilon > 0$.

There are two variants of coin flipping, strong coin flipping and weak coin flipping.

4.1 Strong coin flipping

4.1.1 Definition

In a coin flipping protocol, we call a round of communication one message from Alice to Bob and one message from Bob to Alice. We suppose that Alice always sends the first message and Bob always sends the last message. The protocol is quantum if we allow the parties to send quantum messages and perform quantum operations. A player is honest if he or she follows the protocol. A cheating player can deviate arbitrarily from the protocol but still outputs a value at the end of it.

Definition 4 *A strong coin flipping protocol between two parties Alice and Bob is a protocol where Alice and Bob interact and at the end, Alice outputs a value* $c_A \in \{0, 1, \text{Abort}\}$ *and Bob outputs a value* $c_B \in \{0, 1, \text{Abort}\}$. *If* $c_A = c_B$, *we say that the protocol outputs* $c = c_A = c_B$. *If* $c_A \neq c_B$ *then the protocol outputs* $c = \text{Abort}$.

A strong coin flipping protocol with bias ε *(*$SCF(\varepsilon)$*) has the following properties*

- *If Alice and Bob are honest then* $\Pr[c = 0] = \Pr[c = 1] = 1/2$

- *If Alice cheats and Bob is honest then* $P_A^* = \max\{\Pr[c=0], \Pr[c=1]\} \leq 1/2 + \varepsilon$.
- *If Bob cheats and Alice is honest then* $P_B^* = \max\{\Pr[c=0], \Pr[c=1]\} \leq 1/2 + \varepsilon$

The probabilities P_A^* *and* P_B^* *are called the cheating probabilities of Alice and Bob respectively. The cheating probability of the protocol is defined as* $\max\{P_A^*, P_B^*\}$. *We say that the coin flipping is* perfect *if* $\varepsilon = 0$.

4.1.2 Example

We present here a general construction of Quantum Strong Coin Flipping protocols that can achieve a cheating probability of 3/4. Most quantum strong coin flipping protocols are of this form [ATVY00, Amb01, KN04].

General construction of quantum strong coin flipping protocols

- Alice picks a random $a \in \{0,1\}$, creates some state $|\psi_a\rangle$ in some space $\mathcal{A}_1 \otimes \mathcal{A}_2$ and sends the qubits in space $\mathcal{A}_2$ to Bob. Let's call σ_a the state Alice sends to Bob
- Bob picks a random $b \in \{0,1\}$ and sends b to Alice
- Alice reveals a and sends the qubits in $\mathcal{A}_1$
- Bob checks that the joint state sent by Alice corresponds to $|\psi_a\rangle$ by trying to project this state on $|\psi_a\rangle$. He aborts if this checking procedure fails.
- The outcome of the protocol is $c = a \oplus b$.

Let's analyze this protocol in more detail. If both players are honest then the protocol never Aborts.

Alice cheats and Bob is honest Suppose that Alice wants $c = 0$ as an outcome of the protocol (the same proof will follow for $c = 1$) As a first message, Alice can send any state σ to Bob. Bob then picks a random b. If $b = 0$, Alice wants to reveal $a = 0$. By Uhlmann's Theorem, she can apply an operation on $\mathcal{A}_1$ such that the joint state $|\psi\rangle$ in $\mathcal{A}_1 \otimes \mathcal{A}_2$ satisfies $|\langle\psi|\psi_0\rangle|^2 = F^2(\sigma, \sigma_0)$. Similarly, if $b = 1$, Alice wants to reveal $a = 1$ and she can apply an operation on $\mathcal{A}_1$ such that the joint state $|\psi\rangle$ in $\mathcal{A}_1 \otimes \mathcal{A}_2$ satisfies $|\langle\psi|\psi_1\rangle|^2 = F^2(\sigma, \sigma_1)$. Since b is random, we have

$$P_A^* = \frac{1}{2}\left(F^2(\sigma, \sigma_0) + F^2(\sigma, \sigma_1)\right)$$

We want to remove the dependency on σ to prove an upper bound on Alice's cheating probability. We can use Proposition 8 and show that there is a cheating

strategy such that

$$P_A^* = \frac{1}{2} + \frac{F(\sigma_0, \sigma_1)}{2}$$

Bob cheats and Alice is honest Similarly, we can suppose that Bob wants $c = 0$. This means that he wants to send $b = a$. This is equivalent to saying that Bob wants to guess a when having σ_a. By Proposition 2, we have that

$$P_B^* = \frac{1}{2} + \frac{\Delta(\sigma_0, \sigma_1)}{2}$$

By the Fuchs - Van de Graaf inequalities (Proposition 9), we know that $F(\sigma_0, \sigma_1) \geq 1 - \Delta(\sigma_0, \sigma_1)$. This means in particular that

$$P_A^* \geq 1 - \frac{\Delta(\sigma_0, \sigma_1)}{2}$$

From this, we have $P_A^* + P_B^* \geq 3/2$ and $\max\{P_A^*, P_B^*\} \geq 3/4$ hence any quantum strong coin flipping of this form has cheating probability at least 3/4.

It is actually possible to achieve this bound. Consider the following states:

$$\sigma_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|2\rangle\langle 2|$$
$$\sigma_1 = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|$$

Such protocol corresponds to Ambainis's protocol [Amb01] even though this formulation is due to Kerenidis and Nayak [KN04]. We can easily calculate that $F(\sigma_0, \sigma_1) = \Delta(\sigma_0, \sigma_1) = 1/2$ which gives us directly $P_A^* = P_B^* = 3/4$.

4.2 Weak coin flipping

4.2.1 Definition

A weak coin flipping protocol between two parties Alice and Bob is a protocol where Alice and Bob interact and at the end, Alice outputs a value $c_A \in \{0, 1\}$ and Bob outputs a value $c_B \in \{0, 1\}$. If $c_A = c_B$, we say that the protocol outputs $c = c_A$. If $c_A \neq c_B$ then the protocol outputs $c =$ Abort. The difference with Strong coin flipping is that the players do not Abort. This is because a player that wants to Abort can always declare victory rather than aborting without reducing the security of the protocol.

Definition 5 *A (balanced) weak coin flipping protocol with bias ε ($WCF(1/2, \varepsilon)$) has the following properties*

- *If $c = 0$, we say that Alice wins. If $c = 1$, we say that Bob wins.*
- *If Alice and Bob are honest then* $\Pr[$ *Alice wins* $] = \Pr[$ *Bob wins* $] = 1/2$
- *If Alice cheats and Bob is honest then* $P_A^* = \Pr[$ *Alice wins* $] \leq 1/2 + \varepsilon$
- *If Bob cheats and Alice is honest then* $P_B^* = \Pr[$ *Bob wins* $] \leq 1/2 + \varepsilon$

Similarly, P_A^* and P_B^* are the cheating probabilities of Alice and Bob. The cheating probability of the protocol is defined as $\max\{P_A^*, P_B^*\}$.

We can also define weak coin flipping for the case where the winning probabilities of the two players in the honest case are not equal.

Definition 6 *A weak coin flipping protocol with parameter z and bias ε ($WCF(z,\varepsilon)$) has the following properties.*

- *If $c = 0$, we say that Alice wins. If $c = 1$, we say that Bob wins.*
- *If Alice and Bob are honest then* $\Pr[$ *Alice wins* $] = z$ *and* $\Pr[$ *Bob wins* $] = 1 - z$
- *If Alice cheats and Bob is honest then* $P_A^* = \Pr[$ *Alice wins* $] \leq z + \varepsilon$
- *If Bob cheats and Alice is honest then* $P_B^* = \Pr[$ *Bob wins* $] \leq (1 - z) + \varepsilon$

Unlike strong coin flipping, it is possible to create a quantum weak coin flipping protocol arbitrarily close to optimal. This construction is due to Mochon [Moc07].

Proposition 10 *For any $\varepsilon > 0$, there exists a quantum weak coin flipping protocol with cheating probabilities less than $\frac{1}{2} + \varepsilon$.*

4.2.2 Reformulation of Quantum weak coin flipping protocol

In a quantum protocol, Alice and Bob have an output which they measure to determine the values of c_A, c_B. When using weak-coin flipping in a quantum protocol, it will be useful to keep the quantumness of this output.

We reformulate here the definition of a quantum weak coin flipping to take into account the fact that Alice and Bob are quantum players that perform unitary operations during the protocol and at the end they perform a measurement on a quantum register in order to get their classical output. This will be useful when using quantum weak coin flipping in a quantum protocol as in Chapter 5.

More precisely, let $\mathcal{O}_A$ (resp. $\mathcal{O}_B$) be Alice's (resp. Bob's) one-qubit output register. At the end of the protocol Alice (resp. Bob) has a state ρ_A in $\mathcal{O}_A$ (resp. ρ_B in $\mathcal{O}_B$). They also share some garbage state. The players get their output value by measuring their output qubit in the computational basis. Let ρ_{AB} the joint output state of Alice and Bob in $\mathcal{O}_A \otimes \mathcal{O}_B$. In this setting, we define a weak coin flipping as follows

Definition 7 *A (balanced) weak coin flipping protocol with bias ε ($WCF(1/2,\varepsilon)$) has the following properties*

- *The 0 outcome corresponds to Alice winning. The 1 outcome corresponds to Bob winning.*
- *If Alice and Bob are honest then* $\langle 00|\rho_{AB}|00\rangle = \langle 11|\rho_{AB}|11\rangle = 1/2$
- *If Alice cheats and Bob is honest then* $P_A^* = \langle 0|\rho_B|0\rangle \leq 1/2 + \varepsilon$
- *If Bob cheats and Alice is honest then* $P_B^* = \langle 1|\rho_A|1\rangle \leq 1/2 + \varepsilon$

Notice that Alice's cheating probability depends only on Bob's output. This is because a cheating Alice will always claim that she won, so she wins when Bob outputs 'Alice wins'. We have the same behavior for a cheating Bob.

We also define unbalanced weak coin flipping in this setting.

Definition 8 *A weak coin flipping protocol with parameter z and bias ε ($WCF(z,\varepsilon)$) has the following properties.*

- *The 0 outcome corresponds to Alice winning. The 1 outcome corresponds to Bob winning.*
- *If Alice and Bob are honest then $\langle 00|\rho_{AB}|00\rangle = z$; $\langle 11|\rho_{AB}|11\rangle = 1-z$*
- *If Alice cheats and Bob is honest then $P_A^* = \langle 0|\rho_B|0\rangle \leq z+\varepsilon$*
- *If Bob cheats and Alice is honest then $P_B^* = \langle 1|\rho_A|1\rangle \leq (1-z)+\varepsilon$*

4.2.3 An unbalanced weak coin flipping protocol from balanced weak coin flipping protocol

In the quantum setting, it is known by Mochon's protocol how to build a weak coin flipping protocol which is arbitrarily close to optimal. However, this gives us a balanced weak coin flipping protocol. A natural question is whether we can extend this construction to an unbalanced weak coin flipping protocol.

We show here how to use any almost optimal balanced weak coin flipping protocol to build an almost optimal unbalanced weak coin flipping protocol. This procedure will be purely classical and will use the balanced weak coin flipping as a black box. These unbalanced protocols will be very useful to construct optimal quantum coin flipping and bit commitment protocols.

Our goal is to prove the following proposition

Proposition 11 *Let P be a $WCF(1/2,\varepsilon)$ protocol with N rounds. Then, $\forall z \in [0,1]$ and $\forall k \in \mathbb{N}$, there exists a $WCF(x,\varepsilon_0)$ protocol Q such that:*

- *Q uses $k \cdot N$ rounds.*
- *$|x-z| \leq 2^{-k}$.*
- *$\varepsilon_0 \leq 2\varepsilon$.*

The protocol Q is a sequential composition of the $WCF(1/2,\varepsilon)$ protocol P. In high level, we use P in order to combine two weak coin flipping protocols with parameters z_1 and z_2 into a new protocol with parameter $\frac{z_1+z_2}{2}$. Then, by recursion, for any given z we can create a protocol Q with parameter x that rapidly converges to z. We also prove that the bias of Q is at most 2ε.

Assume we have a $WCF(z_1,\varepsilon_0)$ protocol P_1 and a $WCF(z_2,\varepsilon_0)$ protocol P_2 each with at most M rounds of communication and $z_2 \geq z_1$. We combine them in the following way.

Comb($\mathbf{P_1}, \mathbf{P_2}$)

- Alice and Bob run P.
- If Alice wins, run P_2. If Bob wins, run P_1. If P Aborts then Abort.

Note that this protocol uses at most $N + M$ rounds. We have

Lemma 2 *$Comb(P_1, P_2)$ is a $WCF(\frac{z_1+z_2}{2}, \varepsilon_0 + \varepsilon(z_2 - z_1))$ protocol.*

Proof:

Alice and Bob are honest If Alice and Bob are honest then the protocol never aborts. We have Pr[Alice wins] $= \frac{z_1+z_2}{2}$ and Pr[Bob wins] $= 1 - \frac{z_1+z_2}{2}$.

Alice cheats and Bob is honest Let x = Pr[Alice wins P] ; y = Pr[Bob wins P]; u = Pr[Alice wins P_2 | Alice wins P]; v = Pr[Alice wins P_1 | Bob wins P]. We know the following inequalities concerning these probabilities:

$$x + y \leq 1 \quad x \leq 1/2 + \varepsilon \quad u \leq z_2 + \varepsilon_0 \quad v \leq z_1 + \varepsilon_0$$

Note that the last two inequalities hold, since the biases for the protocols P_1 and P_2 do not increase depending on the outcome of P. We have

$$\begin{aligned}
&\Pr[\text{ Alice wins } Comb(P_1, P_2)] \\
&= \quad x \cdot u + y \cdot v \quad \leq \quad x(z_2 + \varepsilon_0) + (1 - x)(z_1 + \varepsilon_0) \quad = \quad (z_1 + \varepsilon_0) + x(z_2 - z_1) \\
&\leq \quad (z_1 + \varepsilon_0) + (1/2 + \varepsilon)(z_2 - z_1) \qquad \text{since } z_2 \geq z_1 \\
&\leq \quad \frac{z_1 + z_2}{2} + \varepsilon_0 + \varepsilon(z_2 - z_1)
\end{aligned}$$

Bob cheats and Alice is honest Using a similar calculation as in the previous case, we have Pr[Bob wins $Comb(P_1, P_2)$] $\leq \frac{(1-z_2)+(1-z_1)}{2} + \varepsilon_0 + \varepsilon(z_2 - z_1) = 1 - \frac{z_1+z_2}{2} + \varepsilon_0 + \varepsilon(z_2 - z_1)$. ■

We now show the following inductive Lemma

Lemma 3 *Suppose we have a $WCF(1/2, \varepsilon)$ protocol P that uses N rounds of communication. Then $\forall z \in [0, 1]$ and $\forall k \in \mathbb{N}$, we can construct a $WCF(x_1, \varepsilon_0)$ protocol P_1 and a $WCF(x_2, \varepsilon_0)$ protocol P_2 such that*

- *P_1, P_2 each use at most $k \cdot N$ rounds.*
- *$x_1 \leq z \leq x_2$ and $x_2 - x_1 = 2^{-k}$.*
- *$\varepsilon_0 \leq (2 - 2(x_2 - x_1))\varepsilon$.*

Proof: Fix $z \in [0, 1]$. We show this result by induction on k. For $k = 0$, we clearly have a $WCF(0, 0)$ protocol (a protocol where Bob always wins) and a $WCF(1, 0)$ (a protocol where Alice always wins) that use no rounds of communication. We suppose the Lemma is true for k and we show it for $k + 1$.

Let $x_1, x_2, P_1, P_2, \varepsilon_0$ satisfy the above properties for k. Let P' be the $Comb(P_1, P_2)$ protocol and $u = \frac{x_1+x_2}{2}$. P' uses at most $(k+1)N$ rounds and from Lemma 2, we know that P' is a $WCF(u, \varepsilon_0' = \varepsilon_0 + (x_2 - x_1)\varepsilon)$ protocol. From the induction step we have that $\varepsilon_0' \leq (2 - 2(x_2 - x_1))\varepsilon + (x_2 - x_1)\varepsilon \leq (2 - (x_2 - x_1))\varepsilon$. We now distinguish two cases

- If $z \leq u$, consider the protocols P_1 and P'. Each one uses at most $(k+1)N$ rounds. Also, $x_1 \leq z \leq u$ and $u - x_1 = \frac{x_2 - x_1}{2} = 2^{-(k+1)}$. Finally, $\varepsilon_0' \leq (2 - (x_2 - x_1))\varepsilon = (2 - 2(u - x_1))\varepsilon$ which concludes the proof.
- If $z > u$, consider the protocols P' and P_2. Each one uses at most $(k+1)N$ rounds. Also, $u \leq z \leq x_2$ and $x_2 - u = \frac{x_2 - x_1}{2} = 2^{-(k+1)}$. Finally, $\varepsilon_0' \leq (2 - (x_2 - x_1))\varepsilon = (2 - 2(x_2 - u))\varepsilon$ which concludes the proof. ■

In Lemma 3, we have $|x_1 - z| \leq (x_2 - x_1) \leq 2^{-k}$ and $\varepsilon_0 \leq 2\varepsilon$. Hence this Lemma directly implies Proposition 11 by considering $Q = P_1$.

4.3 Optimal quantum strong coin flipping

In this Section, we present a general method on how to use any weak coin-flipping protocol with cheating probability $1/2 + \varepsilon$ in order to construct a strong coin-flipping protocol with cheating probability $1/\sqrt{2} + O(\varepsilon)$. Our protocol uses roughly the same number of rounds as the weak coin flipping protocol. Combining our construction with Mochon's quantum weak coin flipping protocol that achieves arbitrarily small bias, we conclude that it is possible to construct a quantum strong coin flipping protocol with cheating probability arbitrarily close to $\frac{1}{\sqrt{2}}$.

The protocol is classical and uses the weak coin flipping as a subroutine. In other words, in strong coin flipping, the power of quantum really comes from the ability to perform weak coin flipping. If there existed a classical weak coin flipping protocol with arbitrarily small bias, then this would have implied a classical strong coin flipping protocol with cheating probability arbitrarily close to $1/\sqrt{2}$ as well.

4.3.1 A first attempt

Using weak coin flipping in order to perform strong coin flipping is not a new idea. There is a trivial protocol that uses a perfect weak coin flipping and achieves strong coin flipping with cheating probability 3/4: Alice and Bob run the weak coin flipping protocol and whoever wins, flips a random coin $c \in_R \{0, 1\}$.

SCF(3/4) protocol using a perfect weak coin flipping protocol P

- Alice and Bob run the protocol P
- The winner chooses a random $c \in_R \{0,1\}$, and sends c to the other player, c being the outcome of the protocol.

Let us analyze this protocol more closely. Let Alice be dishonest and her desired value for the coin be 0. Her strategy will be to try and win the WCF protocol, which happens with probability 1/2 and then output 0. However, even if she loses the weak coin flipping, there is still a probability 1/2 that the honest Bob will output 0. Hence, Alice's (and by symmetry Bob's) cheating probability is 3/4.

4.3.2 The optimal protocol

In order to reduce this bias, we would like to eliminate the situation where the honest player, after winning the WCF, still helps the dishonest player cheat with probability 1/2. One can try to resolve this problem by having Alice flip and announce her random coin c before running the WCF protocol. In this case: first, Alice announces a bit a. Then, Alice and Bob perform a WCF. If Alice wins the outcome is a; if Bob wins then the outcome is $\overline{a}$.

In this case, Bob never outputs a. However, there is a simple cheating strategy for Alice. If she wants 0, she sets $a = 1$, loses the WCF (which she can potentially do with probability 1) and therefore Bob always outputs 0. Hence, Bob's choice when he wins the WCF must be probabilistic.

Since such protocols are not symmetric, we use an unbalanced weak coin flipping protocol to ensure that the two cheating probabilities are the same. We know how to construct such protocols from balanced protocols using Proposition 11. The coin flipping protocol becomes the following

Quantum Strong Coin Flipping protocol with bias $\frac{1}{\sqrt{2}} + O(\varepsilon)$

1. Alice chooses $a \in_R \{0,1\}$ and sends a to Bob.
2. Alice and Bob perform the $WCF(z,\varepsilon)$ protocol Q
   - If Alice wins Q then honest players output $c_A = c_B = a$
   - If Bob wins Q then he flips a coin b such that $b = a$ with probability p and $b = \overline{a}$ with probability $(1-p)$. He sends b to Alice. In this case, honest players output $c_A = c_B = b$.
   - If Q outputs Abort then Abort

We will now show how to optimize the parameters z and p in order to make the cheating probability of our protocol at most $1/\sqrt{2} + O(\varepsilon)$.

Security analysis of our protocol We calculate the cheating probability of our protocol S that uses a $WCF(z, \varepsilon)$ protocol Q.

Proposition 12 *The protocol S is a strong coin flipping protocol with $N+2$ rounds of communication and cheating probabilities $P_A^* \leq \frac{1}{2-z-\varepsilon}$ and $P_B^* \leq \frac{2-z+\varepsilon}{2}$.*

Proof:
Alice and Bob are honest If both players are honest then they never abort. Moreover, since the protocol is symmetric in 0 and 1, we have $\Pr[c=0] = \Pr[c=1] = 1/2$.
Alice cheats and Bob is honest We prove that $\Pr[c=0] \leq \frac{1}{2-z-\varepsilon}$. By symmetry, the same holds for $\Pr[c=1]$. Since Alice cheats, she can choose arbitrarily between $a=0$ and $a=1$ instead of picking a uniformly at random. Hence, $Pr[c=0] \leq \max\{\Pr[c=0|a=0], \Pr[c=0|a=1]\}$.

- We first calculate $\Pr[c=0|a=0]$.
  Let $x = \Pr[\text{Alice wins } Q|a=0]$ and $y = \Pr[\text{Bob wins } Q|a=0]$. We have $\Pr[c=0|a=0] = x \cdot 1 + y \cdot p$. Note that $x + y \leq 1$ and also $x \leq z + \varepsilon$, since the maximum bias with which Alice can win Q is independent of the value of a. We have

$$\begin{aligned} \Pr[c=0|a=0] &= x \cdot 1 + y \cdot p \leq x + (1-x)p = p + x(1-p) \\ &\leq p + (z+\varepsilon)(1-p) \end{aligned}$$

- We now calculate $\Pr[c=0|a=1]$.
  Let $x = \Pr[\text{Alice wins } Q|a=1]$ and $y = \Pr[\text{Bob wins } Q|a=1]$. We have

$$\Pr[c=0|a=1] = x \cdot 0 + y(1-p) \leq y(1-p) \leq 1-p$$

  which is achievable since Alice could always let Bob win Q.

Since $\Pr[c=0] \leq \max\{\Pr[c=0|a=0], \Pr[c=0|a=1]\}$, we choose p such that the upper bounds for $\Pr[c=0|a=0]$ and $\Pr[c=0|a=1]$ are equal.

$$\begin{aligned} p + (z+\varepsilon)(1-p) &= 1-p \\ p &= \frac{1-z-\varepsilon}{2-z-\varepsilon} \end{aligned}$$

With this value of p, we have

$$Pr[c=0] \leq \max\{\Pr[c=0|a=0], \Pr[c=0|a=1]\} = 1-p \leq \frac{1}{2-z-\varepsilon}$$

Since the protocol is symmetric in 0 and 1, we also have $\Pr[c=1] \leq \frac{1}{2-z-\varepsilon}$ and hence $P_A^* \leq \frac{1}{2-z-\varepsilon}$.

Bob cheats and Alice is honest We prove that $\Pr[c=0] \leq \frac{2-z+\varepsilon}{2}$. By symmetry, the same holds for $\Pr[c=1]$. Alice is honest and picks a uniformly at random. We first have $\Pr[c=0|a=0] \leq 1$. We now upper bound $\Pr[c=0|a=1]$. Let $x = \Pr[\text{Bob wins } Q|a=1]$ and $y = \Pr[\text{Alice wins } Q|a=1]$. We have

$$\Pr[c=0|a=1] \leq x \cdot 1 + y \cdot 0 \leq x \leq 1 - z + \varepsilon$$

Since Alice is honest, we have $\Pr[a=0] = \Pr[a=1] = 1/2$ and hence:

$$\begin{aligned}
\Pr[c=0] &= \Pr[c=0|a=0] \cdot \Pr[a=0] + \Pr[c=0|a=1] \cdot \Pr[a=1] \\
&= \frac{1}{2}\left(\Pr[c=0|a=0] + \Pr[c=0|a=1]\right) \\
&\leq \frac{1}{2} + \frac{1-z+\varepsilon}{2} \\
&= \frac{2-z+\varepsilon}{2}
\end{aligned}$$

Since the protocol is symmetric in 0 and 1, we also have $\Pr[c=1] \leq \frac{2-z+\varepsilon}{2}$ and hence $P_B^* \leq \frac{2-z+\varepsilon}{2}$.

■

4.3.3 Putting it all together

To conclude, we have to optimize z. In the case where there exists an ideal weak coin flipping protocol $WCF(1/2, 0)$, it is easy to see that in order to equalize the cheating probabilities P_A^* and P_B^*, we need to take $z = 2 - \sqrt{2}$. If also our Proposition 11 was ideal, *i.e.* if from P we could create perfectly a $WCF(2-\sqrt{2}, 0)$ protocol Q, then S would have cheating probability exactly $\frac{1}{\sqrt{2}}$.

In general, we need to take care of the small bias ε of the initial $WCF(1/2, \varepsilon)$ protocol P and the error of our Proposition 11. However, we will see that the overall increase in the cheating probability of our protocol S is only $O(\varepsilon)$.

Proposition 13 *If there exists a $WCF(1/2, \varepsilon)$ protocol P that uses N rounds of communication then there exists a strong coin flipping protocol S that uses $2\lceil \log(\frac{1}{\varepsilon}) \rceil \cdot N + 2$ rounds with cheating probability at most $\frac{1}{\sqrt{2}} + \sqrt{2}\varepsilon + o(\varepsilon)$.*

Proof: Starting from the $WCF(1/2, \varepsilon)$ weak coin flipping protocol P with N rounds, we can use Proposition 11 with $k = 2\lceil \log(\frac{1}{\varepsilon}) \rceil$ and construct a $WCF(x, \varepsilon')$ protocol Q with the following properties

- Q uses $2\lceil \log(\frac{1}{\varepsilon}) \rceil \cdot N$ rounds.
- $|x - (2-\sqrt{2})| \leq \varepsilon^2$.
- $\varepsilon' \leq 2\varepsilon$.

We use the protocol Q in the strong coin flipping protocol described in Section 4.3 and by Proposition 12 we a strong coin flipping protocol with

$2\lceil \log(\frac{1}{\varepsilon}) \rceil \cdot N + 2$ rounds and

$$\begin{aligned} P_A^* &= \frac{1}{2-x-\varepsilon'} \leq \frac{1}{\sqrt{2}-2\varepsilon-\varepsilon^2} \leq \frac{1}{\sqrt{2}} + \sqrt{2}\varepsilon + o(\varepsilon) \\ P_B^* &= \frac{2-x+\varepsilon'}{2} \leq \frac{\sqrt{2}+2\varepsilon+\varepsilon^2}{2} = \frac{1}{\sqrt{2}} + \varepsilon + o(\varepsilon) \end{aligned}$$

■

Using Proposition 13 and Mochon's weak coin flipping protocol (Proposition 10) we conclude that

Theorem 1 *For any $\varepsilon > 0$, there exists a strong coin flipping protocol with cheating probability $\frac{1}{\sqrt{2}} + \varepsilon$.*

Last, note that our strong coin flipping protocol uses $O(N \cdot \log(\frac{1}{\varepsilon}))$ rounds, where N is the number of rounds of Mochon's weak coin flipping protocol.

Conclusion

In this Chapter, we presented the first quantum strong coin flipping protocol with a cheating probability arbitrarily close to the optimal value $\frac{1}{\sqrt{2}}$. Our protocol uses as a subroutine the quantum weak coin flipping protocol designed by Mochon which is arbitrarily close to optimal. Note that except when using this quantum weak coin flipping protocol, our entire protocol is classical.

In the next Chapter, we will see another application of Mochon's weak coin flipping protocol: building an optimal quantum bit commitment scheme. In this case however, the protocol will be quantum and not classical.

Chapter 5

Bounds for quantum bit commitment

Bit commitment is a cryptographic primitive that enables two distrustful and far apart parties, Alice and Bob, to simulate a safe. Suppose Alice has a bit b that she wants kept secret. She writes b on a piece of paper and puts the paper into the safe. Bob does not know how to open the safe and hence does not know b. Later on, Alice will want to reveal b. However, Bob wants to make sure that Alice did not change her mind. So he will check that there was only one piece of paper in the safe. This primitive has been widely studied. However, classical bit commitment can only be performed with computational security.

Quantum information allows for bit commitment schemes in the information theoretic setting where no dishonest party can perfectly cheat. Perfect quantum bit commitment is impossible [LC97, May97]. However, unlike the classical case, it is possible to construct partially secure quantum bit commitment. The previously best-known quantum protocol by Ambainis achieves a cheating probability of at most 3/4 [Amb01]. On the other hand, Kitaev showed that no quantum protocol can have cheating probability less than $1/\sqrt{2}$ [Kit03] (his lower bound on coin flipping can be easily extended to bit commitment). Closing this gap has since been an important and open question.

In this Chapter, we provide the optimal bound for quantum bit commitment. We first show a lower bound of approximately 0.739, improving Kitaev's lower bound. We then present an optimal quantum bit commitment protocol which has cheating probability arbitrarily close to 0.739. More precisely, we show how to use any weak coin flipping protocol with cheating probability $1/2+\varepsilon$ in order to achieve a quantum bit commitment protocol with cheating probability $0.739+O(\varepsilon)$. We then use the optimal quantum weak coin flipping protocol described by Mochon [Moc07]. To stress the fact that our protocol uses quantum effects beyond the weak coin flip, we show that any classical bit commitment protocol with access to perfect weak (or strong) coin flipping has cheating probability at least 3/4.

5.1 Definition of quantum bit commitment

Definition 9 *A quantum commitment scheme is an interactive protocol between Alice and Bob with two phases, a Commit phase and a Reveal phase.*

- *In the* commit *phase, Alice interacts with Bob in order to commit to b.*
- *In the* reveal *phase, Alice interacts with Bob in order to reveal b. Bob decides to accept or reject depending on the revealed value of b and his final state. We say that Alice successfully reveals b, if Bob accepts the revealed value.*

We define the following security requirements for the commitment scheme.

- Completeness: *If Alice and Bob are both honest then Alice always successfully reveals the bit b she committed to.*
- Binding property: *For any cheating Alice and for honest Bob, we define Alice's cheating probability as*

$$P_A^* = \frac{1}{2}\left(\Pr[\textit{ Alice successfully reveals } b = 0] + \Pr[\textit{ Alice successfully reveals } b = 1]\right)$$

- Hiding property: *For any cheating Bob and for honest Alice, we define Bob's cheating probability as*

$$P_B^* = \Pr[\textit{ Bob guesses } b \textit{ after the Commit phase }]$$

Remark: The definition of quantum bit commitment we use is the standard one when one studies stand-alone cryptographic primitives. In this setting, quantum bit commitment has a clear relation to other fundamental primitives such as coin flipping and oblivious transfer [ATVY00, Amb01, Kit03, Moc07, CKS10]. Moreover, the study of such primitives sheds light on the physical limits of quantum mechanics and the power of entanglement. Recently there have been some stronger definitions of Quantum Bit Commitment protocols that suit better practical uses (see for example [DFR$^+$07]).

Notice that using our weaker definition of quantum bit commitment only strengthens our lower bound which also holds for the stronger ones.

We now describe more in detail the different steps of a quantum bit commitment protocol. We consider protocols where Alice reveals b at the beginning of the decommit phase. Note that this does not help Bob and can only harm a cheating Alice. Proving a lower bound for such protocols will hence be a lower bound for all bit commitment protocols.

We assume here that Alice and Bob are both honest. Let $\mathcal{A}$ Alice's space and $\mathcal{B}$ Bob's space.

The commit phase: Alice wants to commit to a bit b. Alice and Bob communicate with each other and perform some quantum operations. This can be seen as a joint quantum operation which depends on b. We can suppose wlog that this operation is a quantum unitary U_b^C (by increasing Alice and Bob's quantum space). At the end of the commit phase, Alice and Bob share the quantum state $|\psi_b\rangle$. Let $\sigma_b = \mathrm{Tr}_{\mathcal{A}}|\psi_b\rangle\langle\psi_b|$ be the state that Bob has after the commit phase.

The reveal phase: Alice wants to reveal b to Bob. Alice reveals b at the beginning of the decommit phase. Similarly to the commit phase, we can suppose that the decommit phase is equivalent to Alice and Bob performing a joint unitary U_b^D on their shared state ($|\psi_b\rangle$ if they were honest in the Commit phase). At the end, Bob performs a check to see whether Alice cheated or not. In the honest case, Bob always accepts.

5.2 Lower bound for quantum bit commitment

To prove the lower bound, we will show some generic cheating strategies for Alice and Bob that work for any kind of bit commitment scheme. We will then show that these cheating strategies give a cheating probability of approximately 0.739 for any protocol.

5.2.1 Description of cheating strategies

We denote by $|\psi_b\rangle$ the quantum state Alice and Bob share at the end of the commit phase. Let $\sigma_b = \mathrm{Tr}_{\mathcal{A}}|\psi_b\rangle\langle\psi_b|$ the state that Bob has after the commit phase when Alice honestly commits to bit b.

Bob's cheating strategy The cheating strategy of Bob is the following:

- Perform the Commit phase honestly.
- Guess b by performing on the state at the end of the commit phase the optimal discriminating measurement between σ_0 and σ_1.

First note that an all-powerful Bob can always perform this strategy, since he knows the honest states σ_0 and σ_1 and can hence compute and perform the optimal measurement. Let us analyze this strategy. We know [Hel67] that Bob can guess b with probability $\frac{1}{2} + \frac{\Delta(\sigma_0,\sigma_1)}{2}$ and hence

$$P_B^* \geq \frac{1}{2} + \frac{\Delta(\sigma_0, \sigma_1)}{2}$$

Alice's cheating strategy The cheating strategy of Alice is the following

- Perform a quantum strategy so that at the end of the commit phase, Bob has the state $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$.
- In order to reveal a specific value b, send b then apply a local quantum operation such that the actual joint state of the protocol, $|\phi_b\rangle$, satisfies $|\langle\phi_b|\psi_b\rangle| = F(\sigma_+, \sigma_b)$. Perform the rest of the reveal phase honestly.

First note that an all-powerful Alice can perform this strategy. An honest Alice has a strategy to make Bob's state after the commit phase equal to σ_b for both $b = 0$ and $b = 1$. A cheating Alice creates a qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Conditioned on 0 (resp. 1), she applies the strategy that will give Bob the state σ_0 (resp. σ_1). By doing this Bob's state at the end of the commit phase is exactly σ_+. Moreover, by Uhlmann's theorem, Alice can compute and perform the local unitary in the beginning of the reveal phase to create a state $|\phi_b\rangle$ that satisfies $|\langle\phi_b|\psi_b\rangle| = F(\sigma_+, \sigma_b)$.

For the analysis, since Bob accepts b with probability 1 when the joint state of the protocol is $|\psi_b\rangle$, he accepts with probability at least $|\langle\phi_b|\psi_b\rangle|^2 = F^2(\sigma_+, \sigma_b)$ when the joint state of the protocol is $|\phi_b\rangle$. From this cheating strategy, we have that

$$P_A^* \geq \frac{1}{2}\left(F^2(\sigma_+, \sigma_0) + F^2(\sigma_+, \sigma_1)\right)$$

5.2.2 Showing the Lower Bound

We have the following bounds for cheating Alice and cheating Bob.

$$P_A^* \geq \frac{1}{2}\left(F^2(\sigma_+, \sigma_0) + F^2(\sigma_+, \sigma_1)\right)$$
$$P_B^* \geq \frac{1}{2} + \frac{\Delta(\sigma_0, \sigma_1)}{2}$$

We now use the following inequality that will be proved in the next section

Proposition 14 *Let σ_0, σ_1 any two quantum states. Let $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$. We have*

$$\frac{1}{2}\left(F^2(\sigma_+, \sigma_0) + F^2(\sigma_+, \sigma_1)\right) \geq \left(1 - (1 - \frac{1}{\sqrt{2}})\Delta(\sigma_0, \sigma_1)\right)^2.$$

Let $t = \Delta(\sigma_0, \sigma_1)$. From the above Proposition, we have the following bounds.

$$P_A^* \geq \frac{1}{2}\left(F^2(\sigma_+, \sigma_0) + F^2(\sigma_+, \sigma_1)\right) \geq \left(1 - (1 - \frac{1}{\sqrt{2}})t\right)^2$$
$$P_B^* \geq \frac{1}{2} + \frac{\Delta(\sigma_0, \sigma_1)}{2} = \frac{1+t}{2}$$

We get an upper bound on the optimal cheating probability by equalizing these two bounds, *ie.*

$$\left(1 - (1 - \frac{1}{\sqrt{2}})t\right)^2 = \frac{1+t}{2}$$

Notice that the same cheating probabilities appeared in the analysis of a weak coin flipping protocol in [KN04]. Solving the equation gives $t \approx 0.4785$ and hence we have

Theorem 2 *In any quantum bit commitment protocol with cheating probabilities P_A^* and P_B^* we have* $\max\{P_A^*, P_B^*\} \geq 0.739$.

5.2.3 Proof of the fidelity Lemma

In this Section, we show Proposition 14.

Proof of Proposition 14**:** We will prove this Lemma in three steps. Let σ_0, σ_1 two quantum states and let $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$.

Step 1 We first consider the states $\rho_0 = \frac{1}{2}|0\rangle\langle 0| \otimes \sigma_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \sigma_1$ and $\rho_+ = \frac{1}{2}|0\rangle\langle 0| \otimes \sigma_+ + \frac{1}{2}|1\rangle\langle 1| \otimes \sigma_+$. We compute the trace distance and fidelity of these states

$$\Delta(\rho_0, \rho_+) = \frac{1}{2}\left(\Delta(\sigma_0, \sigma_+) + \Delta(\sigma_1, \sigma_+)\right) = \frac{1}{2}\Delta(\sigma_0, \sigma_1) \tag{5.1}$$

In order to calculate the fidelity we note first that $\rho_+^{\frac{1}{2}} = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| \otimes \sigma_+^{\frac{1}{2}} + |1\rangle\langle 1| \otimes \sigma_+^{\frac{1}{2}}\right)$. From the definition of fidelity we have

$$\begin{aligned}
F(\rho_0, \rho_+) &= tr\left(\sqrt{\rho_+^{\frac{1}{2}}\rho_0\rho_+^{\frac{1}{2}}}\right) \\
&= tr\left(\sqrt{\frac{1}{4}|0\rangle\langle 0| \otimes \sigma_+^{\frac{1}{2}}\sigma_0\sigma_+^{\frac{1}{2}} + \frac{1}{4}|1\rangle\langle 1| \otimes \sigma_+^{\frac{1}{2}}\sigma_1\sigma_+^{\frac{1}{2}}}\right) \\
&= tr\left(\frac{1}{2}|0\rangle\langle 0| \otimes \sqrt{\sigma_+^{\frac{1}{2}}\sigma_0\sigma_+^{\frac{1}{2}}} + \frac{1}{2}|1\rangle\langle 1| \otimes \sqrt{\sigma_+^{\frac{1}{2}}\sigma_1\sigma_+^{\frac{1}{2}}}\right) \\
&= \frac{1}{2}tr\left(\sqrt{\sigma_+^{\frac{1}{2}}\sigma_0\sigma_+^{\frac{1}{2}}}\right) + \frac{1}{2}tr\left(\sqrt{\sigma_+^{\frac{1}{2}}\sigma_1\sigma_+^{\frac{1}{2}}}\right) \\
&= \frac{1}{2}\left(F(\sigma_0, \sigma_+) + F(\sigma_1, \sigma_+)\right)
\end{aligned}$$

Hence, by Cauchy-Schwarz we conclude that

$$F^2(\rho_0, \rho_+) \leq \frac{1}{2}F^2(\sigma_0, \sigma_+) + \frac{1}{2}F^2(\sigma_1, \sigma_+) \tag{5.2}$$

Step 2 Consider the POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho_0 E_i)$ and $q_i = tr(\rho_+ E_i)$ such that $F(\rho_0, \rho_+) = \sum_i \sqrt{p_i q_i}$ (Prop. 5). We consider the states $D_0 = \sum_i p_i |i\rangle\langle i|$ and $D_+ = \sum_i q_i |i\rangle\langle i|$. For the trace distance and fidelity of these states, we have

$$\Delta(D_0, D_+) = \frac{1}{2}\sum_i |p_i - q_i| \leq \Delta(\rho_0, \rho_+) = \frac{1}{2}\Delta(\sigma_0, \sigma_1) \quad \text{by Prop. 3, 1 and Eq. 5.1} \tag{5.3}$$

$$F(D_0, D_+) = F(\rho_0, \rho_+) = \sum_i \sqrt{p_i q_i} \tag{5.4}$$

Step 3 Let us define k such that $k/2 = \Delta(D_0, D_+)$. We now consider the states $T_0 = k|0\rangle\langle 0| + (1-k)|2\rangle\langle 2|$ and $T_+ = \frac{k}{2}|0\rangle\langle 0| + \frac{k}{2}|1\rangle\langle 1| + (1-k)|2\rangle\langle 2|$. We calculate the trace distance and fidelity of these states

$$\Delta(T_0, T_+) = \frac{k}{2} = \Delta(D_0, D_+) \leq \frac{\Delta(\sigma_0, \sigma_1)}{2} \tag{5.5}$$

$$F(T_0, T_+) = \left(1 - k + \frac{k}{\sqrt{2}}\right) \geq \left(1 - (1 - \frac{1}{\sqrt{2}})\Delta(\sigma_0, \sigma_1)\right) \tag{5.6}$$

The only thing remaining is to show that $F(T_0, T_+) \leq F(D_0, D_+)$. To prove this, we construct a completely positive trace preserving operation Q such that $Q(T_0) = D_0$ and $Q(T_+) = D_+$. We can then conclude using Proposition 7.

We define $D_1 = \sum_i r_i |i\rangle\langle i|$ with $p_i + r_i = 2q_i$. This means that $D_+ = \frac{1}{2}D_0 + \frac{1}{2}D_1$ and $\Delta(D_0, D_1) = k$.

Let $A = \{i : p_i \geq r_i\}$ and $B = \{i : p_i < r_i\}$. Let $w_i = \min\{p_i, r_i\}$ We consider the following Q

$$\begin{aligned}
Q(|0\rangle\langle 0|) &= \sum_{i\in A} \frac{1}{k}(p_i - r_i)|i\rangle\langle i| \\
Q(|1\rangle\langle 1|) &= \sum_{i\in B} \frac{1}{k}(r_i - p_i)|i\rangle\langle i| \\
Q(|2\rangle\langle 2|) &= \sum_i \frac{1}{1-k} w_i |i\rangle\langle i| \\
Q(|i\rangle\langle j|) &= 0 \quad \text{for } i \neq j
\end{aligned}$$

Since $\Delta(D_0, D_1) = k$, we have in particular that $\sum_i w_i = 1-k$; $\sum_{i\in A}(p_i - r_i) = \sum_{i\in B}(r_i - p_i) = k$ (see Proposition 3). Q is hence a completely positive trace preserving operation. We now have:

$$\begin{aligned}
Q(T_0) &= k\sum_{i\in A} \frac{1}{k}(p_i - r_i)|i\rangle\langle i| + (1-k)\sum_i \frac{1}{1-k} w_i |i\rangle\langle i| \\
&= \sum_{i\in A}(p_i - r_i)|i\rangle\langle i| + \sum_i w_i |i\rangle\langle i| \\
&= \sum_{i\in A}(p_i - r_i + r_i)|i\rangle\langle i| + \sum_{i\in B} p_i |i\rangle\langle i| \\
&= \sum_i p_i |i\rangle\langle i| = D_0
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
Q(T_+) &= \frac{k}{2}\sum_{i\in A} \frac{1}{k}(p_i - r_i)|i\rangle\langle i| + \frac{k}{2}\sum_{i\in B} \frac{1}{k}(r_i - p_i)|i\rangle\langle i| + (1-k)\sum_i \frac{1}{1-k} w_i |i\rangle\langle i| \\
&= \sum_{i\in A} \frac{p_i - r_i}{2}|i\rangle\langle i| + \sum_{i\in B} \frac{r_i - p_i}{2}|i\rangle\langle i| + \sum_i w_i |i\rangle\langle i| \\
&= \sum_{i\in A}(r_i + \frac{p_i - r_i}{2})|i\rangle\langle i| + \sum_{i\in B}(p_i + \frac{r_i - p_i}{2})|i\rangle\langle i| \\
&= \sum_i q_i |i\rangle\langle i| = D_+
\end{aligned}$$

From this, we conclude that

$$F(D_0, D_+) = F(Q(T_0), Q(T_+)) \geq F(T_0, T_+). \tag{5.7}$$

Putting everything together, we have using equations 5.2,5.4,5.6,5.7

$$\begin{aligned}\frac{1}{2}\left(F^2(\sigma_0,\sigma_+)+F^2(\sigma_1,\sigma_+)\right) &\geq F^2(\rho_0,\rho_+)\\ &\geq F^2(D_0,D_+)\\ &\geq F^2(T_0,T_+)\\ &\geq \left(1-(1-\frac{1}{\sqrt{2}})\Delta(\sigma_0,\sigma_1)\right)^2\end{aligned}$$

■

5.3 Upper Bound for quantum bit commitment

In this section we describe and analyze a protocol that proves the optimality of our bound.

Theorem 3 *There exists a quantum bit commitment protocol that uses a weak coin flipping protocol with cheating probability* $1/2+\epsilon$ *as a subroutine and achieves cheating probabilities less than* $0.739+O(\epsilon)$.

Our protocol is a quantum improvement of the following simple protocol that achieves cheating probability 3/4. Alice commits to bit b by preparing the state $1/\sqrt{2}(|bb\rangle+|22\rangle)$ and sending the second qutrit to Bob. In the reveal phase, she sends the first qutrit and Bob checks that the pure state is the correct one. It is not hard to prove that both Alice and Bob can cheat with probability 3/4 [Amb01, KN04]. The main idea in order to reduce the cheating probabilities for both players is the following: first we increase a little bit the amplitude of the state $|22\rangle$ in this superposition. This decreases the cheating probability of Bob. However, now Alice can cheat even more. To remedy this, we use the quantum procedure of a weak coin flipping so that Alice and Bob jointly create the above initial state (with the appropriate amplitudes) instead of having Alice create it herself. We present now the details of the protocol.

5.3.1 The protocol

Optimal Quantum Bit Commitment

Commit phase, Step 1 Alice and Bob perform an unbalanced weak coin flipping procedure (without measuring the final outcome), where Alice wins with probability $1-p$ and Bob with probability p. As we said, we can think of this procedure as a big unitary operation that creates a joint pure state in the space of Alice and Bob. Moreover, Alice and Bob have each a special 1-qubit register that they can measure at the end of the protocol in order to read the outcome of the weak coin flipping. Here, we assume that they do not measure anything and that at the end Alice sends back to Bob all her garbage qubits. In other words, in the honest case, Alice and Bob share the following state at the end of the weak coin protocol

$$|\Omega\rangle = \sqrt{p}|L\rangle_{\mathcal{A}} \otimes |L, G_L\rangle_{\mathcal{B}} + \sqrt{1-p}|W\rangle_{\mathcal{A}} \otimes |W, G_W\rangle_{\mathcal{B}}$$

where W corresponds to the outcome "Alice wins" and L corresponds to the outcome "Alice loses". The spaces $\mathcal{A}, \mathcal{B}$ correspond to Alice's and Bob's private quantum space. The garbage states $|G_W\rangle, |G_L\rangle$ are known to both players.

Commit phase, Step 2 After the end of the weak coin flipping procedure, Alice does the following. Conditioned on her qubit being W, she creates two qutrits in the state $|22\rangle$ and sends the second to Bob. Conditioned on her qubit being L, she creates two qutrits in the state $|bb\rangle$ where b is the bit she wants to commit to and sends the second to Bob. If the players are both honest, they share the following state:

$$|\Omega_b\rangle = \sqrt{p}|L, b\rangle_{\mathcal{A}} \otimes |L, b, G_L\rangle_{\mathcal{B}} + \sqrt{1-p}|W, 2\rangle_{\mathcal{A}} \otimes |W, 2, G_W\rangle_{\mathcal{B}}$$

Reveal phase In the reveal phase, Alice sends b and all her remaining qubits in space $\mathcal{A}$ to Bob. Bob checks that he has the state $|\Omega_b\rangle$.

5.3.2 Analysis of the above protocol

If Alice and Bob are both honest then Alice always successfully reveals the bit b she committed to.

Cheating Bob Bob is not necessarily honest in the weak coin flipping protocol, however the weak coin flipping has small bias ϵ. Since Alice is honest, Bob has all the qubits expect the one qubit which is in Alice's output register. At the end of the first step of the Commit phase, Alice and Bob share a state

$$|\Omega^*\rangle = \sqrt{p'}|L\rangle_{\mathcal{A}}|\Psi_L\rangle_{\mathcal{B}} + \sqrt{1-p'}|W\rangle_{\mathcal{A}}|\Psi_W\rangle_{\mathcal{B}}$$

for some states $|\Psi_L\rangle, |\Psi_W\rangle$ held by Bob. Recall that the outcome L in Alice's output register corresponds to the outcome where Alice loses the weak coin flipping protocol. Hence, for any cheating Bob, since our coin flipping has bias

ε, we have $p' \leq p + \varepsilon$. At the end of the commit phase, depending on Alice's committed bit b, the joint state is

$$|\Omega_b^*\rangle = \sqrt{p'}|L, b\rangle_{\mathcal{A}}|b, \Psi_L\rangle_{\mathcal{B}} + \sqrt{1-p'}|W, 2\rangle_{\mathcal{A}}|2, \Psi_W\rangle_{\mathcal{B}}$$

and Bob's density matrix is

$$\sigma_b^* = p'|b, \Psi_L\rangle\langle b, \Psi_L| + (1-p')|2, \Psi_W\rangle\langle 2, \Psi_W|.$$

By Proposition 2, we have

$$P_B^* = \Pr[\text{ Bob guesses } b] \leq \frac{1}{2} + \frac{\Delta(\sigma_0^*, \sigma_1^*)}{2} = \frac{1}{2} + \frac{p'}{2} \leq \frac{1+p}{2} + \frac{\varepsilon}{2}$$

Cheating Alice Let σ_b be Bob's reduced state at the end of the commit phase when both players are honest. Let $|\overline{x}\rangle = |L, x, G_L\rangle$ for $x \in \{0, 1\}$ and $|\overline{2}\rangle = |W, 2, G_W\rangle$. We have

$$\sigma_b = p|\overline{b}\rangle\langle\overline{b}| + (1-p)|\overline{2}\rangle\langle\overline{2}|$$

Let ξ be Bob's state at the end of the commit phase for a cheating Alice. Let $r_i = \langle\overline{i}|\xi|\overline{i}\rangle$ for $i \in \{0, 1, 2\}$. From the characterization of the fidelity in Proposition 7, we have that

$$F(\xi, \sigma_b) \leq \sqrt{pr_b} + \sqrt{(1-p)r_2}$$

From standard analysis of bit commitment protocol (for example [KN04]), we have using Uhlmann's Theorem that

$$\begin{aligned} P_A^* &\leq \frac{1}{2}\left(F^2(\xi, \sigma_0) + F^2(\xi, \sigma_1)\right) \\ &\leq \frac{1}{2}\left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 + \frac{1}{2}\left(\sqrt{pr_1} + \sqrt{(1-p)r_2}\right)^2 \end{aligned}$$

In order to get a tight bound for the above expression, we use here the property of the weak coin flipping. Recall that $|\overline{2}\rangle = |W, 2, G_W\rangle$ has its first register as W (this corresponds to Alice winning the coin flip). On the other hand, $|\overline{0}\rangle$ and $|\overline{1}\rangle$ have L as their first register, corresponding to the case where Bob wins. For any cheating Alice, she can win the weak coin flip with probability smaller than $1 - p + \varepsilon$ and hence this means in particular that $r_2 \leq 1 - p + \varepsilon$. Moreover, $r_0 + r_1 + r_2 \leq 1$. For $\varepsilon < p(1 - \frac{1}{2-p})$, we show that this quantity is maximal when r_2 is maximal and $r_0 = r_1 = (p - \varepsilon)/2$ (proven in the next Section). This gives us

$$P_A^* \leq \left(\sqrt{p \cdot \frac{p-\varepsilon}{2}} + \sqrt{(1-p)(1-p+\varepsilon)}\right)^2 \leq \left(1 - (1 - \frac{1}{\sqrt{2}})p\right)^2 + O(\varepsilon)$$

Putting it all together Except for the terms in ε, we obtain exactly the same quantities as in our lower bound. By equalizing these cheating probabilities, we have

$$\max\{P_A^*, P_B^*\} \approx 0.739 + O(\varepsilon)$$

which proves Theorem 3 Since we can have ε arbitrarily close to 0 (Proposition 10) and we can have an unbalanced weak coin flipping protocol with probability arbitrarily close to p (Proposition 11), we conclude that our protocol is arbitrarily close to optimal, and hence we proved Theorem 3.

5.3.3 Proof of $r_0 = r_1$ and r_2 maximal in the quantum lower bound

In this Section, we show the following:

Proposition 15 *Let*

$$P_A^* \leq \frac{1}{2}\left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 + \frac{1}{2}\left(\sqrt{pr_1} + \sqrt{(1-p)r_2}\right)^2$$

with the constraints: $r_0, r_1, r_2 \geq 0$, $r_0 + r_1 + r_2 \leq 1$ *and* $r_2 \leq 1 - p + \varepsilon$ *for* $\varepsilon < p(1 - \frac{1}{2-p})$. *This cheating probability is maximized for* $r_0 = r_1 = \frac{p-\varepsilon}{2}$ *and* $r_2 = 1 - p + \varepsilon$.

Proof: First note that the maximal cheating probability is achieved for $r_0 + r_1 + r_2 = 1$ since this cheating probability is increasing in r_0, r_1, r_2.

We first show that $r_0 = r_1$. Let's fix r_2. This means that $S = r_0 + r_1 = 1 - r_2$ is fixed. Let $u = \sqrt{(1-p)r_2}$. We have

$$P_A^* \leq f(r_0) = \frac{1}{2}\left(\sqrt{pr_0} + u\right)^2 + \frac{1}{2}\left(\sqrt{p(S - r_0)} + u\right)^2.$$

Taking the derivative, we have

$$\begin{aligned} &= \frac{1}{2}\left(p + \frac{u\sqrt{p}}{\sqrt{r_0}} - p - \frac{u}{\sqrt{p}}\sqrt{S - r_0}\right) \\ &= \frac{u\sqrt{p}}{2}\left(\frac{1}{\sqrt{r_0}} - \frac{1}{\sqrt{S - r_0}}\right) \end{aligned}$$

We have $f'(r_0) > 0$ for $r_0 < S/2$; $f'(r_0) = 0$ for $r_0 = S/2$; $f'(r_0) < 0$ for $r_0 > S/2$. This means that the maximum of f is achieved for $r_0 = S/2$ *i.e.* $r_0 = r_1$.

We now show that $r_2 = 1 - p + \varepsilon$ gives the maximal cheating probability if ε is not too big. Since P_A^* is maximal for $r_0 = r_1$ and for $r_0 + r_1 + r_2 = 1$, we have

$$\begin{aligned} P_A^* &\leq \frac{1}{2}\left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 + \frac{1}{2}\left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 \\ &\leq \left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 \\ &\leq \left(\sqrt{p(\frac{1 - r_2}{2})} + \sqrt{(1-p)r_2}\right)^2 = g(r_2) \end{aligned}$$

Again, we take the derivative of g.

$$g'(r_2) = \left(-\frac{\sqrt{p}}{\sqrt{2(1-r_2)}} + \frac{\sqrt{1-p}}{\sqrt{r_2}}\right) \cdot \left(\sqrt{p(\frac{1 - r_2}{2})} + \sqrt{(1-p)r_2}\right)$$

From this, we have

$$\begin{aligned} g'(r_2) \geq 0 \Leftrightarrow & \left(-\frac{\sqrt{p}}{\sqrt{2(1-r_2)}} + \frac{\sqrt{1-p}}{\sqrt{r_2}} \right) \geq 0 \\ \Leftrightarrow & \sqrt{\frac{p}{2(1-r_2)}} \leq \sqrt{\frac{1-p}{r_2}} \\ \Leftrightarrow & pr_2 \leq 2(1-r_2)(1-p) \\ \Leftrightarrow & r_2 \leq 1 - \frac{p}{2-p} \end{aligned}$$

For $\varepsilon < p(1 - \frac{1}{2-p})$, we have $1 - p + \varepsilon < 1 - \frac{p}{2-p}$, so when $\varepsilon < p(1 - \frac{1}{2-p})$, $g(r_2)$ is always increasing when $r_2 \leq 1 - p + \varepsilon$ and is maximal when $r_2 = 1 - p + \varepsilon$, which concludes the proof. ■

5.4 Proof of the classical lower bound

In this Section, we show a 3/4 lower bound for classical bit commitment schemes when players additionally have the power to perform perfect (strong or weak) coin-flipping. This will show that unlike strong coin flipping, quantum and classical bit commitment are not alike in the presence of weak coin flipping.

We first describe such protocols in Section 5.4.1. In Section 5.4.2, we construct a cheating strategy for Alice and Bob for these protocols such that one of the players can cheat with probability at least 3/4.

5.4.1 Description of a classical bit commitment protocol with perfect coin flips

We describe classical bit commitment schemes when players additionally have the power to perform perfect (strong or weak) coin-flipping. The way we deal with the coin is the following: when Alice and Bob are honest, they always output the same random value c and both players know this value. We can suppose equivalently that a random coin c is given publicly to both Alice and Bob each time they perform coin flipping. We describe any BC protocol with coins as follows:

- Alice and Bob have some private randomness R_A and R_B respectively.
- *Commit phase:* Alice wants to commit to some value x. Let N the number of rounds of the commit phase. For $i = 1$ to N: Alice sends a message a_i, Bob sends a message b_i, Alice and Bob flip a coin and get a public $c_i \in_R \{0, 1\}$.
- *Reveal phase:* Alice wants to decommit to some value y ($= x$ if Alice is honest).

  1. Alice first reveals y. This is a restriction for the protocol but showing a lower bound for such protocols will show a lower bound for all protocols since this can only limit Alice's cheating possibilities without helping Bob.

2. Let M the number of rounds of the reveal phase. For $i = 1$ to M: Alice sends a message a'_i, Bob sends a message b'_i, Alice and Bob flip a coin and get a public $c'_i \in_R \{0,1\}$.
3. Bob has an accepting procedure Acc to decide whether he accepts the revealed bit or whether he aborts (if Bob catches Alice cheating).

We denote the commit phase transcript by $t_C = (a_1, b_1, c_1, \ldots, a_N, b_N, c_N)$. If Alice and Bob are honest, then we can write $t_C = T_C(R_A, R_B, c, x)$ where T_C is a function fixed by the protocol that takes as input Alice and Bob's private coins R_A, R_B, the outcomes of the public coin flips $c = (c_1, \ldots, c_N)$ as well as the bit x Alice wants to commit to and outputs a commit phase transcript t_C. If we can write $t_C = T_C(R_A, R_B, c, x)$ for some R_A, R_B, c, x, we say that t_C is an honest commit phase transcript.

Similarly, we define the decommit phase transcript by $t_D = (a'_1, b'_1, c'_1, \ldots, a'_M, b'_M, c'_M)$. If Alice and Bob are honest, we can write $t_D = T_D(R_A, R_B, c', y, t_C)$, where T_D is a function fixed by the protocol that takes as input Alice and Bob's private coins R_A, R_B, the outcomes of the public coin flips $c' = (c'_1, \ldots, c'_M)$, the bit y Alice reveals as well as the commit phase transcript t_C and outputs a reveal phase transcript t_D. If we can write $t_D = T_D(R_A, R_B, c', y, t_C)$ for some R_A, R_B, c', y and some honest commit phase transcript t_C, we say that t_D is an honest reveal phase transcript.

Whether Bob accepts at the end of the protocol depends on both transcripts t_C, t_D of the commit and reveal phase, the bit y Alice reveals as well as Bob's private coins. We write that $Acc(t_C, t_D, y, R_B) = 1$ when Bob accepts.

Note that in the honest case, Bob always accepts Alice's decommitment. This means that we can transform Alice's honest strategy in the reveal phase to a deterministic strategy which will also be always accepted. This fact will be useful in the proof.

5.4.2 Proof of the classical lower bound

In this Section, we construct cheating strategies for Alice and Bob such that one of the players will be able to cheat with probability greater than 3/4. We only consider cheating strategies where Alice and Bob are honest during the coin flips so again, they will be modeled as public and perfectly random coins. Moreover, Alice and Bob will always be honest during the commit phase.

Before describing the cheating strategies we need some definitions. More particularly, we consider a cheating Alice who cheats during the reveal phase by following a deterministic strategy A^*. For a fixed honest commit phase transcript t_C, we can write the transcript of the reveal phase as a function of A^*, R_B, c', y, t_C, more precisely $T^*_D(A^*, R_B, c', y, t_C)$.

Definition 10 *We say that R_B is consistent with t_C if and only if there exist R_A, c, x such that $t_C = T_C(R_A, R_B, c, x)$.*

Definition 11 *Let t_C an honest commit phase transcript. We say that $t_C \in A_y$ if and only if*

$\exists A^*$ *s.t.* $\forall c'$ *and* $\forall R_B$ *consistent with* $t_C, Acc(t_C, T^*_D(A^*, R_B, c', y, t_C), y, R_B) = 1$

Intuitively, $t_C \in A_y$ means that if Alice and Bob output an honest commit phase transcript t_C, there is a deterministic strategy A^* for Alice that allows her to reveal y without Bob aborting, independently of Bob's private coins R_B. Since there is always a deterministic honest strategy for Alice in the reveal phase (when Alice and bob have been honest in the commit phase), we have

$$\forall\ R_A, R_B, c, x \qquad t_C = T_C(R_A, R_B, c, x) \in A_x$$

Notice also that for any honest commit phase transcript t_C, both players Alice and Bob can compute whether $t_C \in A_u$ for both $u = 0$ and $u = 1$.

Definition 12 *We define the probability*

$p_u = \Pr[t_C = T_C(R_A, R_B, c, u) \in A_{\overline{u}}]$ *where the probability is taken over uniform* R_A, R_B, c.

Consider that Bob is honest. p_u *is the probability that if Alice behaves honestly in the commit phase and commits to* u*, she has a deterministic cheating strategy to reveal* $\overline{u}$ *which always succeeds (independently of* c', R_B*).*

We can now describe and analyze our cheating strategies for Alice and Bob and prove our theorem

Theorem 4 *For any classical bit commitment protocol with access to public perfect coins, one of the players can cheat with probability at least* $3/4$.

Proof: Let us fix a bit commitment protocol. We describe cheating strategies for Alice and Bob.

Cheating Alice

- Commit phase: Alice picks $x \in_R \{0,1\}$ and she honestly commits to x during the commit phase.
- Reveal phase: if Alice wants to reveal x, she just remains honest during the reveal phase. By completeness of the protocol, this strategy succeeds with probability 1. If Alice wants to reveal $\overline{x}$, we know by definition of p_x that she succeeds with probability at least p_x. This gives us:

  $$P_A^* \geq \frac{1}{2} + \frac{p_x}{2}$$

  since Alice chooses x at random, we have:

  $$P_A^* \geq \frac{1}{2} + \frac{p_0 + p_1}{4}$$

Cheating Bob As Alice, Bob is honest in the commit phase. Let x the bit Alice committed to. Since Alice and Bob are honest the commit-phase transcript is $t_C = T_C(R_A, R_B, c, x)$ for uniformly random R_A, R_B, c. As said before, we know that $t_C \in A_x$.

At the end of the commit phase, Bob wants to guess the bit x Alice commits to and he performs the following strategy: if $t_C \in A_0 \cap A_1$ he guesses x at random. If $\exists!\ u$ s.t. $t_C \notin A_u$ he guesses $x = \overline{u}$.

We know that Bob succeeds in cheating with probability $1/2$ if $t_C \in A_{\overline{x}}$ and with probability 1 if $t_C \notin A_{\overline{x}}$. This gives us $P_B^* \geq p_x \cdot \frac{1}{2} + (1 - p_x) \cdot 1 = 1 - \frac{p_x}{2}$. Since again, Alice's bit x is uniformly random, we have

$$P_B^* \geq 1 - \frac{p_0 + p_1}{4}$$

Putting it all together Taking Alice and Bob cheating probabilities together, we have
$P_A^* + P_B^* \geq 3/2$ which gives $\max\{P_A^*, P_B^*\} \geq 3/4$. ■

5.5 Conclusion

In this Chapter, we presented new bounds for Quantum bit Commitment, improving both the lower bound and the upper bound. In the end, we got a lower bound of 0.739 and an upper bound of $0.739 + \varepsilon$ for any $\varepsilon > 0$ which is a construction of a quantum bit commitment arbitrarily close to optimal.

The lower bound we obtained is of different flavor than the one found by Kiteav for coin flipping. While Kitaev's lower bound uses semi-definite programming, our bound just reasons on quantum states.

Like the optimal quantum coin flipping, this protocol uses Mochon's quantum weak coin flipping as a subroutine. We show however, that in addition to weak coin flipping, one also needs quantum effects elsewhere, since we show that any classical bit commitment with access to perfect coin flips cannot achieve better cheating probabilities than 3/4.

Chapter 6

Bounds for quantum Oblivious transfer

In this Chapter, we quantitatively study the bias of quantum oblivious transfer protocols. More precisely, we construct a bit commitment protocol that uses oblivious transfer as a subroutine and show a relation between the cheating probabilities of the OT protocol and the ones of the bit commitment protocol. Then, using the lower bound for quantum bit commitment from Chapter 5, we derive a non-trivial lower bound (albeit weaker) on the cheating probabilities for OT. More precisely we prove the following theorem.

Theorem 5 *In any quantum oblivious transfer protocol, we have*

$$\max\{A_{OT}, B_{OT}\} \geq 0.58$$

Moreover, in Section 6.4 we describe a simple 1-out-of-2 random-OT protocol and analyze the cheating probabilities of Alice and Bob.

Theorem 6 *There exists a quantum oblivious transfer protocol such that* $A_{OT} = B_{OT} = \frac{3}{4}$.

6.1 Definitions

In the literature, many different variants of oblivious transfer have been considered. We consider two variants of quantum oblivious transfer and for completeness we show that they are equivalent with respect to the bias ε.

Definition 13 (Random Oblivious Transfer) *A 1-out-of-2 quantum random oblivious transfer protocol with bias ε, denoted here as random-OT, is a protocol between Alice and Bob such that:*

- *Alice outputs two bits (x_0, x_1) or Abort and Bob outputs two bits (b, y) or Abort*
- *If Alice and Bob are honest, they never Abort, $y = x_b$, Alice has no information about b and Bob has no information about $x_{\overline{b}}$. Also, x_0, x_1, b are uniformly random bits.*

- $A_{OT} := \sup\{\Pr[\textit{Alice guesses } b \textit{ and Bob does not Abort}]\} = \frac{1}{2} + \varepsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob guesses } (x_0, x_1) \textit{ and Alice does not Abort}]\} = \frac{1}{2} + \varepsilon_B$
- *The bias of the protocol is defined as* $\varepsilon := \max\{\varepsilon_A, \varepsilon_B\}$

where the suprema are taken over all cheating strategies for Alice and Bob.

Note that this definition is slightly different from usual definitions because we want the exact value of the cheating probabilities and not only an upper bound. This is because we consider both lower bounds and upper bounds for *OT* protocols but we could have equivalent results using the standard definitions.

An important issue is that we quantify the security against a cheating Bob as the probability that he can guess (x_0, x_1). One can imagine a security definition where Bob's guessing probability is not for (x_0, x_1), but for example for $x_0 \oplus x_1$ or any other function $f(x_0, x_1)$. Since we are mostly interested in lower bounds, we believe our definition is the most appropriate one, since a lower bound on the probability of guessing (x_0, x_1) automatically yields a lower bound on the probability of guessing any $f(x_0, x_1)$.

We now define a second notion of *OT* where the values (x_0, x_1) and b are Alice's and Bob's inputs respectively and show the equivalence between the two notions.

Definition 14 (Oblivious Transfer) *A 1-out-of-2 quantum oblivious transfer protocol with bias* ε*, denoted here as OT, is a protocol between Alice and Bob such that:*

- *Alice has input* $x_0, x_1 \in \{0,1\}$ *and Bob has input* $b \in \{0,1\}$*. At the beginning of the protocol, Alice has no information about* b *and Bob has no information about* (x_0, x_1)
- *At the end of the protocol, Bob outputs* y *or Abort and Alice can either Abort or not*
- *If Alice and Bob are honest, they never Abort,* $y = x_b$*, Alice has no information about* b *and Bob has no information about* $x_{\overline{b}}$
- $A_{OT} := \sup\{\Pr[\textit{Alice guesses } b \textit{ and Bob does not Abort}]\} = \frac{1}{2} + \varepsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob guesses } (x_0, x_1) \textit{ and Alice does not Abort}]\} = \frac{1}{2} + \varepsilon_B$
- *The bias of the protocol is defined as* $\varepsilon := \max\{\varepsilon_A, \varepsilon_B\}$

where the suprema are taken over all cheating strategies for Alice and Bob.

6.2 Equivalence between the different notions of Oblivious Transfer

We show the equivalence between *OT* and random-*OT* with respect to the bias ε. First, note that a random-*OT* is a special case of *OT*, since in the definition of *OT* there is no restriction on how the inputs are chosen, and hence they can be chosen uniformly at random.

Proposition 16 *Let P an OT protocol with bias ε. We can construct a random-OT protocol Q with bias ε using P.*

Proof: The construction of the OT protocol Q is pretty straightforward:

1. Alice picks $x_0, x_1 \in_R \{0,1\}$ uniformly at random and Bob picks $b \in_R \{0,1\}$ uniformly at random.
2. Alice and Bob perform the OT protocol P where Alice inputs x_0, x_1 and Bob inputs b. Let y be Bob's output. Note that at this point, Alice has no information about b and Bob has no information about (x_0, x_1).
3. Alice and Bob abort in Q if and only if they abort in P. Otherwise, the outputs of protocol Q are (x_0, x_1) for Alice and (b, y) for Bob.

The outcomes of Q are uniformly random bits since Alice and Bob choose their inputs uniformly at random. All the other requirements that make Q an OT protocol with bias ε are satisfied because P is an OT protocol with bias ε. ■

We now prove how to go from a random-OT to an OT protocol.

Proposition 17 *Let P a random-OT protocol with bias ε_P. We can construct an OT protocol Q with bias $\varepsilon_Q = \varepsilon_P$ using P.*

Proof: Let P a random-OT protocol with bias ε_P. Consider the following protocol Q:

1. Alice has inputs X_0, X_1 and Bob has an input B.
2. Alice and Bob run protocol P and output (x_0, x_1) for Alice and (b, y) for Bob.
3. Bob sends $r = b \oplus B$ to Alice. Let $x'_c = x_{c \oplus r}$, for $c \in \{0,1\}$.
4. Alice sends to Bob (s_0, s_1) where $s_c = x'_c \oplus X_c$ for $c \in \{0,1\}$. Let $y' = y \oplus s_B$.
5. Alice and Bob abort in Q if and only if they abort in P. Otherwise, the output of the protocol is y' for Bob.

Note that this procedure is entirely classical. We now show that our protocol is an OT protocol with inputs with bias ε. First, note that the values x'_c are known by Alice and the value y' is known by Bob. Also, notice that $x'_B = x_{B \oplus r} = x_b$.

- Alice and Bob are honest:
  By definition we have $y = x_b$. Then, we have $y' = y \oplus s_B = x_b \oplus s_B = x'_B \oplus s_B = X_B$. Moreover, Alice knows r but has no information about b and hence she has no information about $B = b \oplus r$. Bob knows (s_0, s_1) and r but has no information about $x_{\bar{b}}$, hence he has no information about $X_{\bar{B}} = x'_{\bar{B}} \oplus s_{\bar{B}} = x'_{\bar{b} \oplus r} \oplus s_{\bar{b} \oplus r} = x_{\bar{b}} \oplus s_{\bar{b} \oplus r}$.
- Cheating Alice:
  Alice picks r and $B = b \oplus r$. Hence

$$\begin{aligned} A_{OT}(Q) &= \sup\{\Pr[\text{Alice guesses } B \text{ and Bob does not Abort}]\} \\ &= \sup\{\Pr[\text{Alice guesses } b \text{ and Bob does not Abort}]\} = A_{OT}(P). \end{aligned}$$

- Cheating Bob: Bob picks a random r, sends r to Alice and then Alice picks (s_0, s_1). We have $X_c = x'_c \oplus s_c = x_{c\oplus r} \oplus s_c$ so it is equivalent for Bob to guess (X_0, X_1) and (x_0, x_1). Hence

$$\begin{aligned} B_{OT}(Q) &= \sup\{\Pr[\text{Bob guesses } (X_0, X_1) \text{ and Alice does not Abort}]\} \\ &= \sup\{\Pr[\text{Bob guesses } (x_0, x_1) \text{ and Alice does not Abort}]\} = B_{OT}(P). \end{aligned}$$

We can now conclude for the biases

$$\varepsilon_Q = \max\{A_{OT}(Q), B_{OT}(Q)\} - \frac{1}{2} = \max\{A_{OT}(P), B_{OT}(P)\} - \frac{1}{2} = \varepsilon_P.$$

■

6.3 Lower bound for quantum oblivious transfer

6.3.1 From quantum oblivious transfer to quantum bit commitment

In this section we prove that the bias of any random-OT protocol, and hence any OT protocol, is bounded below by a constant. We start from a random-OT protocol and first show how to construct a bit commitment protocol. Then, we prove a relation between the cheating probabilities of the bit commitment and those in the random-OT protocol. Last, we use the lower bounds for quantum bit commitment from Chapter 5.

We create a bit commitment protocol from a random-OT protocol as follows.

Bit Commitment Protocol via random-OT

- *Commit phase*: We invert the roles of Alice and Bob. Bob is the one who commits. He wants to commit to a bit a. Alice and Bob perform the OT protocol such that Alice has (x_0, x_1) and Bob has (b, x_b). Bob sends $a \oplus b$ to Alice.
- *Decommit phase*: Bob reveals b and $y = x_b$ to Alice. If x_b from Bob is consistent with Alice's bits then Alice accepts. Otherwise Alice aborts.

We now analyze how much Alice and Bob can cheat in the bit commitment protocol and compare these quantities to the bias of the random-OT protocol. Let A_{OT}, B_{OT} the cheating probabilities for the quantum oblivious transfer protocol and A_{BC}, B_{BC} the cheating probabilities for the resulting quantum bit commitment protocol. Our goal is to show the following:

Proposition 18

$$A_{OT} \leq A_{BC} \ ; \ B_{OT} \leq f(BC) \qquad \textit{where } f(x) = x(2x-1)^2$$

Proof:

Let $\neg\perp_A^{BC}$ (resp. $\neg\perp_B^{BC}$) denote the event "Alice (resp. Bob) does not abort during the entire bit commitment protocol". Let $\neg\perp_A^{OT}$ (resp. $\neg\perp_B^{OT}$) denote the event "Alice (resp. Bob) does not abort during the random-OT subroutine".

Cheating Alice By definition, A_{OT} is the optimal probability of Alice guessing b in the random-OT protocol without Bob aborting and A_{BC} is the optimal probability of Alice guessing a in the bit commitment protocol without Bob aborting. Since Alice knows $c := a \oplus b$, the probability of Alice guessing a in the bit commitment protocol is the same as the probability of her guessing b in the random-OT protocol. Thus $A_{OT} = A_{BC}$.

Cheating Bob By definition, B_{OT} is the optimal probability of Bob learning both bits in the random-OT protocol without Alice aborting. Thus,

$$\begin{aligned} B_{OT} &= \sup\{\Pr[\text{ (Bob guesses } (x_0, x_1)) \wedge \neg\perp_A^{OT}]\} \\ &= \sup\{\Pr[\neg\perp_A^{OT}] \cdot \Pr[\text{ (Bob guesses } (x_0, x_1))|\neg\perp_A^{OT}]\}. \end{aligned}$$

where the suprema are taken over all strategies for Bob.

If Bob wants to reveal 0 in the bit commitment protocol (a similar argument works if he wants to reveal 1), then first, Alice must not abort in the random-OT protocol and second, Bob must send $b = c$ as well as the correct x_c such that Alice does not abort in the last round of the bit commitment protocol. This is equivalent to saying that Bob succeeds if he guesses x_c and Alice does not abort in the random-OT protocol. Since Bob randomly chooses which bit he wants to reveal, we can write the probability of Bob cheating as

$$\begin{aligned} B_{BC} &= \max\left\{\frac{1}{2}\Pr[(\text{Bob guesses } x_0) \wedge \neg\perp_A^{OT}] + \frac{1}{2}\Pr[(\text{Bob guesses } x_1) \wedge \neg\perp_A^{OT}]\right\} \\ &= \max\left\{\Pr[\neg\perp_A^{OT}] \cdot \left(\frac{1}{2}\Pr[(\text{Bob guesses } x_0)|\neg\perp_A^{OT}] + \frac{1}{2}\Pr[(\text{Bob guesses } x_1)|\neg\perp_A^{OT}]\right)\right\}. \end{aligned}$$

Notice that we use "max" instead of "sup" above. This is because an optimal strategy exists for every coin flipping protocol. This is a consequence of strong duality in the semidefinite programming formalism of [Kit03], see [ABDR04] for details.

Let us now fix Bob's optimal cheating strategy in the bit commitment protocol. For this strategy, let $p = \Pr[(\text{Bob guesses } x_0)|\neg\perp_A^{OT}]$, $q = \Pr[(\text{Bob guesses } x_1)|\neg\perp_A^{OT}]$ and $a = \frac{p+q}{2}$. Note that, without loss of generality, we can assume that Bob's measurements are projective measurements. This can be done by increasing the dimension of Bob's space. Also, Alice has a projective measurement on her space to determine the bits (x_0, x_1).

We use the following lemma to relate B_{BC} and B_{OT}.

Lemma 4 (Learning-In-Sequence Lemma) *Let $p, q \in [1/2, 1]$. Let Alice and Bob share a joint pure state. Suppose Alice performs on her space a projective measurement $M = \{M_{x_0,x_1}\}_{x_0,x_1 \in \{0,1\}}$ to determine the values of (x_0, x_1). Suppose there is a projective measurement $P = \{P_0, P_1\}$ on Bob's space that allows him to guess bit x_0 with probability p and a projective measurement $Q = \{Q_0, Q_1\}$ on his space that allows him to guess bit x_1 with probability q. Then, there exists a measurement on Bob's space that allows him to guess (x_0, x_1) with probability at least $a(2a-1)^2$ where $a = \frac{p+q}{2}$.*

We postpone the proof of this lemma to Subsection 6.3.2.

We now construct a cheating strategy for Bob for the OT protocol: Run the optimal cheating bit commitment strategy and look at Bob's state after step 1 conditioned on $\neg\perp_A^{OT}$. Note that this event happens with nonzero probability in the optimal bit commitment strategy since otherwise the success probability is 0. The optimal bit commitment strategy gives measurements that allow Bob to guess x_0 with probability p and x_1 with probability q. Bob uses these measurements and the procedure of Lemma 4 to guess (x_0, x_1). Let m be the probability he guesses (x_0, x_1). From Lemma 4, we have that $m \geq a(2a-1)^2$. By definition of B_{OT} and B_{BC}, we have:

$$m = \Pr[\text{ (Bob guesses } (x_0,x_1))|\neg\perp_A^{OT}] \leq \frac{B_{OT}}{\Pr[\neg\perp_A^{OT}]} \quad \text{and} \quad a = \frac{B_{BC}}{\Pr[\neg\perp_A^{OT}]}.$$

This gives us

$$\frac{B_{OT}}{\Pr[\neg\perp_A^{OT}]} \geq \frac{B_{BC}}{\Pr[\neg\perp_A^{OT}]}\left(2\frac{B_{BC}}{\Pr[\neg\perp_A^{OT}]}-1\right)^2 \implies B_{OT} \geq B_{BC}\left(2B_{BC}-1\right)^2,$$

where the implication holds since $B_{BC} \geq 1/2$. ■

Using this Proposition and the lower bound for quantum bit commitment, we can show our lower bound

Theorem 7 *In any quantum oblivious transfer protocol, at least one of the players can cheat with probability* 0.58.

Proof: We use $A_{BC} = A_{OT}$ and $f(B_{BC}) \leq B_{OT}$ (where $f(x) = x(2x-1)^2$) from Proposition 18. From Chapter 5, we have that for any quantum bit commitment scheme, there exists a parameter $t \in [0,1]$ such that

$$A_{BC} \geq (1-(1-\frac{1}{\sqrt{2}})t)^2 \quad ; \quad B_{BC} \geq \frac{1}{2}+\frac{t}{2}$$

We immediately have that there exists a parameter $t \in [0,1]$ such that

$$A_{OT} \geq (1-(1-\frac{1}{\sqrt{2}})t)^2 \quad ; \quad B_{OT} \geq f(\frac{1}{2}+\frac{t}{2}) = t^2(\frac{1}{2}+\frac{t}{2})$$

We get the lower bound by equalizing A_{OT} and B_{OT} which gives us

$$\begin{aligned}(1-(1-\frac{1}{\sqrt{2}})t)^2 &= t^2(\frac{1}{2}+\frac{t}{2}) \\ t &\approx 0.8046 \\ \max\{A_{OT}, B_{OT}\} &\geq 0.5841\end{aligned}$$

■

6.3.2 Proof of the Learning-In-Sequence Lemma

A few claims

Claim 1 *Let $|X\rangle$ be a pure state, Q a projection, and $|Y\rangle$ a pure state such that $Q|Y\rangle = |Y\rangle$. Then we have*

$$\|Q|X\rangle\|_2^2 \geq |\langle X|Y\rangle|^2.$$

Proof: Using Cauchy-Schwarz we have

$$|\langle X|Y\rangle|^2 = |\langle X|Q|Y\rangle|^2 \leq \| Q|X\rangle \|_2^2 \| |Y\rangle \|_2^2 = \| Q|X\rangle \|_2^2.$$

■

Claim 2 *Suppose $\theta, \theta' \in [0, \pi/4]$. If $|\langle\psi|\phi\rangle| \geq \cos(\theta)$ and $|\langle\phi|\xi\rangle| \geq \cos(\theta')$ then*

$$|\langle\psi|\xi\rangle| \geq \cos(\theta + \theta').$$

Proof: Define the angle between two pure states $|\psi\rangle$ and $|\phi\rangle$ as $A(\psi, \phi) := \arccos|\langle\psi|\phi\rangle|$. This is a metric (see [NC00] page 413). Thus we have

$$\arccos|\langle\psi|\xi\rangle| = A(\psi, \xi) \leq A(\psi, \phi) + A(\phi, \xi) = \arccos|\langle\psi|\phi\rangle| + \arccos|\langle\phi|\xi\rangle| \leq \theta + \theta'.$$

Taking the cosine of both sides yields the result. ■

Claim 3 *Let $\theta, \rho \in [0, \pi/4]$. Then*

$$\cos(\theta + \rho) \geq \cos^2(\theta) + \cos^2(\rho) - 1.$$

Proof: Wlog suppose that $\theta \geq \rho$. Consider the function

$$f(\theta) = \cos(\theta + \rho) - \cos^2(\theta) + \sin^2(\rho)$$

for fixed ρ. Taking its derivative we get

$$f'(\theta) = -\sin(\theta + \rho) + \sin(2\theta)$$

which is nonnegative for $\theta \in [\rho, \pi/4]$. Since $f(\rho) = 0$, we conclude that $f(\theta) \geq 0$ for $\theta \in [\rho, \pi/4]$ which gives the desired result. ■

The Learning-in-Sequence Lemma follows from the following simple geometric result.

Lemma 5 *Let $|\psi\rangle$ be a pure state and let $\{C, I - C\}$ and $\{D, I - D\}$ be two projective measurements such that*

$$\cos^2(\theta) := \| C|\psi\rangle \|_2^2 \geq 1/2 \quad \text{and} \quad \cos^2(\theta') := \| D|\psi\rangle \|_2^2 \geq 1/2.$$

Then we have

$$\| DC|\psi\rangle \|_2^2 \geq \cos^2(\theta)\cos^2(\theta + \theta').$$

Proof: Define the following states

$$|X\rangle := \frac{C|\psi\rangle}{\| C|\psi\rangle \|_2}, \quad |X'\rangle := \frac{(I - C)|\psi\rangle}{\| (I - C)|\psi\rangle \|_2}, \quad |Y\rangle := \frac{D|\psi\rangle}{\| D|\psi\rangle \|_2}, \quad |Y'\rangle := \frac{(I - D)|\psi\rangle}{\| (I - D)|\psi\rangle \|_2}.$$

Then we can write $|\psi\rangle = \cos(\theta)|X\rangle + e^{i\alpha}\sin(\theta)|X'\rangle$ and $|\psi\rangle = \cos(\theta')|Y\rangle + e^{i\beta}\sin(\theta')|Y'\rangle$ with $\alpha, \beta \in \mathbb{R}$. Then we have

$$\begin{aligned} \| DC|\psi\rangle \|_2^2 &= \cos^2(\theta)\| D|X\rangle \|_2^2 \\ &\geq \cos^2(\theta)|\langle Y|X\rangle|^2 \quad \text{using Claim 1} \\ &\geq \cos^2(\theta)\cos^2(\theta + \theta') \quad \text{using Claim 2.} \end{aligned}$$

■

We now prove Lemma 4.

Proof: Let $|\Omega\rangle_{\mathcal{AB}}$ be the joint pure state shared by Alice and Bob, where $\mathcal{A}$ is the space controlled by Alice and $\mathcal{B}$ the space controlled by Bob.

Let $M = \{M_{x_0,x_1}\}_{x_0,x_1\in\{0,1\}}$ be Alice's projective measurement on $\mathcal{A}$ to determine her outputs x_0, x_1. Let $P = \{P_0, P_1\}$ be Bob's projective measurement that allows him to guess x_0 with probability $p = \cos^2(\theta)$ and $Q = \{Q_0, Q_1\}$ be Bob's projective measurement that allows him to guess x_1 with probability $q = \cos^2(\theta')$. These measurements are on $\mathcal{B}$ only. Recall that $a = \frac{p+q}{2} = \frac{\cos^2(\theta)+\cos^2(\theta')}{2}$. We consider the following projections on $\mathcal{AB}$:

$$C = \sum_{x_0,x_1} M_{x_0,x_1} \otimes P_{x_0} \quad \text{and} \quad D = \sum_{x_0,x_1} M_{x_0,x_1} \otimes Q_{x_1}.$$

C (resp. D) is the projection on the subspace where Bob guesses correctly the first bit (resp. the second bit) after applying P (resp. Q).

A strategy for Bob to learn both bits is simple: apply the two measurements P and Q one after the other, where the order in which P and Q are applied is random.

The projection on the subspace where Bob guesses (x_0, x_1) when applying P then Q is

$$E = \sum_{x_0,x_1} M_{x_0,x_1} \otimes Q_{x_1}P_{x_0} = DC.$$

Similarly, the projection on the subspace where Bob guesses (x_0, x_1) when applying Q then P is

$$F = \sum_{x_0,x_1} M_{x_0,x_1} \otimes P_{x_0}Q_{x_1} = CD.$$

With this strategy Bob can guess both bits with probability

$$\begin{aligned}
& \frac{1}{2}\left(||E|\Omega\rangle||_2^2 + ||F|\Omega\rangle||_2^2\right) \\
= \; & \frac{1}{2}\left(||DC|\Omega\rangle||_2^2 + ||CD|\Omega\rangle||_2^2\right) \\
\geq \; & \frac{1}{2}\left(\cos^2(\theta) + \cos^2(\theta')\right)\cos^2(\theta+\theta') \quad \text{using Lemma 5} \\
\geq \; & \frac{1}{2}\left(\cos^2(\theta) + \cos^2(\theta')\right)\left(\cos^2(\theta) + \cos^2(\theta') - 1\right)^2 \quad \text{using Claim 3} \\
= \; & a(2a-1)^2.
\end{aligned}$$

Note that we can use Lemma 5 since Bob's optimal measurement to guess x_0 and x_1 succeeds for each bit with probability at least 1/2. ■

6.4 A Two-Message Protocol With Bias 1/4

We present in this section a random-OT protocol with bias 1/4. This also implies, as we have shown, an OT protocol with inputs with the same bias.

Random Oblivious Transfer Protocol

1. Bob chooses $b \in_R \{0,1\}$ and creates the state $|\phi_b\rangle = \frac{1}{\sqrt{2}}|bb\rangle + \frac{1}{\sqrt{2}}|22\rangle$.
   He sends half of this state to Alice.
2. Alice chooses $x_0, x_1 \in_R \{0,1\}$ and applies the unitary $|a\rangle \to (-1)^{x_a}|a\rangle$,
   where $x_2 := 0$.
3. Alice returns the qutrit to Bob who now has the state $|\psi_b\rangle := \frac{(-1)^{x_b}}{\sqrt{2}}|bb\rangle + \frac{1}{\sqrt{2}}|22\rangle$.
4. Bob performs on the state $|\psi_b\rangle$ the measurement $\{\Pi_0 = |\phi_b\rangle\langle\phi_b|, \Pi_1 := |\phi'_b\rangle\langle\phi'_b|,$
   $I - \Pi_0 - \Pi_1\}$, where $|\phi'_b\rangle := \frac{1}{\sqrt{2}}|bb\rangle - \frac{1}{\sqrt{2}}|22\rangle$.
   If the outcome is Π_0 then $x_b = 0$, if it is Π_1 then $x_b = 1$, otherwise he aborts.

It is clear that Bob can learn x_0 or x_1 perfectly. Moreover, note that if he sends half of the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ then he can also learn $x_0 \oplus x_1$ perfectly (although in this case he does not learn either of x_0 or x_1). We now show that it is impossible for him to perfectly learn both x_0 and x_1 and also that his bit is not completely revealed to a cheating Alice.

Theorem 8 *In the protocol described above, we have* $A_{OT} = B_{OT} = \frac{3}{4}$.

Proof: We analyze the cheating probabilities of each party.

Cheating Alice

Define Bob's space as $\mathcal{B}$ and let $\sigma_b := \mathrm{Tr}_{\mathcal{B}}(|\phi_b\rangle\langle\phi_b|)$ denote the two reduced states Alice may receive in the first message. Then, the optimal strategy for Alice to learn b is to perform the optimal measurement to distinguish between σ_0 and σ_1. In this case, she succeeds with probability

$$\frac{1}{2} + \frac{1}{4}\| \sigma_0 - \sigma_1 \|_{tr} = \frac{3}{4},$$

(see for example [KN04]). Alice's optimal measurement is, in fact, a measurement in the computational basis. If she gets outcome $|0\rangle$ or $|1\rangle$ then she knows b with certainty. If she gets outcome $|2\rangle$ then she guesses. Notice also, that even after this measurement she can return the measured qutrit to Bob and the outcome of Bob's measurement will always be either Π_0 or Π_1. Hence, Bob will never abort.

Cheating Bob

Bob wants to learn both bits (x_0, x_1). We now describe a general strategy for Bob:

- Bob creates $|\psi\rangle = \sum_i \alpha_i |i\rangle_{\mathcal{A}}|e_i\rangle_{\mathcal{B}}$ and sends the $\mathcal{A}$ part to Alice. The $|e_i\rangle$'s are not necessarily orthogonal but $\sum_i |\alpha_i|^2 = 1$.
- Alice applies U_{x_0,x_1} on her part and sends it back to Bob. He now has the state $|\psi_{x_0,x_1}\rangle = \sum_i \alpha_i (-1)^{x_i}|i\rangle|e_i\rangle$ recalling that $x_2 := 0$.

At the end of the protocol, Bob applies a two-outcome measurement on $|\psi_{x_0,x_1}\rangle$ to get his guess for (x_0, x_1).

From this strategy, we create another strategy with the same cheating probability where Bob sends a pure state. We define this strategy as follows:

- Bob creates $|\psi'\rangle = \sum_i \alpha_i |i\rangle_{\mathcal{A}}$ and sends the whole state to Alice.
- Alice applies U_{x_0,x_1} on her part and sends it back to Bob. He now has the state $|\psi'_{x_0,x_1}\rangle = \sum_i \alpha_i (-1)^{x_i} |i\rangle$ recalling that $x_2 := 0$.
- Bob applies the unitary $U : |i\rangle|0\rangle \to |i\rangle|e_i\rangle$ to $|\psi'_{x_0,x_1}\rangle|0\rangle$ and obtains $|\psi_{x_0,x_1}\rangle$.

To determine (x_0, x_1), Bob applies the same measurement as in the original strategy.

Clearly both strategies have the same success probability. When Bob uses the second strategy, Alice and Bob are unentangled after the first message and Alice sends back a qutrit to Bob. We use the following Claim originally due to Nayak.

Proposition 19 ([DW09] following [Nay99]) *Suppose we have a classical random variable X, uniformly distributed over $[n] = \{1, \ldots, n\}$. Let $x \to |\phi_x\rangle$ be some encoding of $[n]$, where $|\phi_x\rangle$ is a pure state in a d-dimensional space. Let $P_1, \ldots, P_n$ be the measurement operators applied for decoding; these sum to the d-dimensional identity operator. Then the probability of correctly decoding in case $X = x$ is*

$$p_x = ||P_x|\phi_x\rangle||^2 \leq \mathrm{Tr}(P_x).$$

The expected success probability is

$$\frac{1}{n}\sum_{x=1}^{n} p_x \leq \frac{1}{n}\sum_{x=1}^{n} \mathrm{Tr}(P_x) = \frac{1}{n}\mathrm{Tr}\left(\sum_{x=1}^{n} P_x\right) = \frac{1}{n}\mathrm{Tr}(I) = \frac{d}{n}.$$

Using this Claim, we directly have

$$\Pr[\text{Bob correctly guesses } (x_0, x_1)] \leq 3/4.$$

Note that there is a strategy for Bob to achieve 3/4. Bob wants to learn both bits (x_0, x_1). Suppose he creates the state

$$|\psi\rangle := \frac{1}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle + \frac{1}{\sqrt{3}}|2\rangle$$

and sends it to Alice. The state he receives is

$$|\psi_{x_0,x_1}\rangle := \frac{1}{\sqrt{3}}(-1)^{x_0}|0\rangle + \frac{1}{\sqrt{3}}(-1)^{x_1}|1\rangle + \frac{1}{\sqrt{3}}|2\rangle.$$

Then, Bob performs a projective measurement in the 4-dimensional basis $\{|\Psi_{x_0,x_1}\rangle : x_0, x_1 \in \{0,1\}\}$ where

$$|\Psi_{x_0,x_1}\rangle := \frac{1}{2}(-1)^{x_0}|0\rangle + \frac{1}{2}(-1)^{x_1}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}(-1)^{x_0 \oplus x_1}|3\rangle.$$

The probability that Bob guesses the two bits x_0, x_1 correctly is

$$\sum_{x_0,x_1} \frac{1}{4} \Pr[\text{Bob guesses } (x_0, x_1)] = \sum_{x_0,x_1} \frac{1}{4} |\langle \Psi_{x_0,x_1} | \psi_{x_0,x_1} \rangle|^2 = \frac{3}{4}.$$

Note that in our protocol Alice never aborts. ■

One possibility to improve this bound would be to use the techniques used in the previous Chapter. By using quantum weak coin flipping, one could try to control the first state sent by Bob. Unfortunately, this approach does not work for this protocol since both cheating players want to decrease the quantity $\langle 2|\rho|2\rangle$ if Bob's state sent is ρ. To ensure that this quantity remains the same with a cheating player, we would need quantum perfect strong coin flipping which is impossible.

6.5 Conclusion

In this chapter, we presented a way to reduce quantum oblivious transfer to quantum bit commitment and showed a relationship between the cheating probabilities of the two protocols. We use this relationship and our lower bound on quantum bit commitment to derive a lower bound for quantum oblivious transfer of 0.58. We also constructed a quantum oblivious transfer protocol with cheating probability 3/4. However, there is still a gap between the lower and the upper bound. The main open question here is to have tight bounds for quantum oblivious transfer.

Chapter 7

Device independent quantum coin flipping and quantum bit commitment

In this Chapter, we extend our study of quantum bit commitment and quantum coin flipping to the device independent model. We show the following

Theorem 9 *There exists a device-independent quantum bit commitment protocol with cheating probability* 0.854 *and a quantum coin flipping protocol with cheating probability* 0.836.

7.1 The device independent model

A quantum protocol is said to be device-independent if the reliability of its implementation can be guaranteed without making any assumptions regarding the internal workings of the underlying apparatus. For example, the measurement device could be flawed, or the quantum states one sends are different than the expected ones. No matter what imperfections exist, we want to guarantee the security of the protocol. This is of interest since lately, there has been some work on how to exploit such imperfections in order to break existing quantum cryptosystems [XQL10, LWW$^+$10].

In the device independent model, we get the following kind of security:

- If the apparatus used is working according to the specifications, the protocol will succeed
- If the apparatus is flawed, or even fabricated by an adversary, the protocol will detect it and the protocol will abort. Note that there is no a priori way to check whether some given apparatus is flawed or not (the checking device could also be flawed).

So far, device independent protocols have been proposed for quantum key distribution [AGM06, ABG$^+$07, MY03, BHK05], random number generation [Col09, PAM$^+$10], state estimation [BLM$^+$09], and the self-testing of quantum computers [MMMO06].

It is not a priori clear, whether the scope of the device independent approach can be extended to cover cryptographic problems with distrustful parties. In particular, this setting presents us with a novel challenge: Whereas in device independent quantum key-distribution Alice and Bob will cooperate to estimate the amount of nonlocality present, for protocols in the distrustful cryptography model, honest parties can rely only on themselves.

In this chapter we show that protocols in this model are indeed amenable to a device independent formulation. We show how to use quantum non-locality and more precisely the GHZ paradox to build a device independent bit commitment protocol where Alice's cheating probability is $P_A^* \leq 0.854$ and Bob's cheating probability is $P_B^* \leq 3/4$. We then use this protocol to construct a device independent coin flipping protocol with cheating probability 0.836.

Device independent formulation

In our device-independent formulation, we assume that each honest party has one or several devices which are viewed as 'black boxes'. Each box allows for a classical input $s_i \in \{0,1\}$, and produces a classical output $r_i \in \{0,1\}$ (the index i designates the box).

We suppose that the boxes are shielded *i.e.* they cannot communicate with each other. Notice that this can be done experimentally without knowing what is inside the box by appropriately confining it.

The probabilities of the outputs given the inputs for an honest party are hence expressed for n boxes as

$$P(\mathbf{r_1}, \ldots, \mathbf{r_n} | \mathbf{s_1}, \ldots, \mathbf{s_n}) = \mathrm{Tr}\big(\rho(\bigotimes_i \Pi_{r_i|s_i})\big)$$

where ρ is some joint quantum state and $\Pi_{r_i|s_i}$ is a POVM element corresponding to inputting s_i in box i and obtaining the outcome r_i. Apart from this constraint we impose no restrictions on the boxes' behavior. In particular, we allow a dishonest party to choose the state ρ (which she can entangle with her system) and the POVM elements $\Pi_{r_i|s_i}$ for the other party's boxes.

The above assumption amounts to the most general modeling of boxes that

1. satisfy the laws of quantum theory
2. are such that the physical process yielding the output r_i in box i depends solely on the input s_i, i.e. the boxes cannot communicate with one another. It is also implicit in our analysis that no unwanted information can enter or exit an honest party's laboratory.

In a fully distrustful setting, where the devices too cannot be trusted, these conditions can be satisfied by shielding the boxes. Notice also that we do not rely on the fact that the boxes are far away. This observation is important because relativistic causality is by itself sufficient for perfect bit commitment and coin flipping [Ken99a, Ken99b].

7.2 Device independent quantum bit commitment

7.2.1 The GHZ paradox

Our protocol is based on the Greenberger-Horne-Zeilinger (GHZ) paradox [GHZ89, Mer90].

The GHZ paradox

- setting: We consider three boxes A, B, and C with binary inputs, s_A, s_B and s_C, and outputs r_A, r_B and r_C, respectively. The boxes do not communicate with each other.
- goal: If the inputs satisfy $s_A \oplus s_B \oplus s_C = 1$, we want $r_A \oplus r_B \oplus r_C = s_A s_B s_C \oplus 1$.

This relation can be guaranteed if the three boxes implement measurements on a three-qubit GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, where $s_i = 0$ (resp. $s_i = 1$) corresponds to measuring in the $\{|+\rangle, |-\rangle\}$ basis (resp. in the $\{|0\rangle, |1\rangle\}$ basis). In contrast, for classical boxes this relation can only be satisfied with $\frac{3}{4}$ probability at most.

We will also use the CHSH game

The CHSH game

- setting: We consider two boxes A, B that do not communicate with binary inputs s_A, s_B and binary outputs r_A, r_B respectively.
- goal: $r_A \oplus r_B = s_A \cdot s_B$

In the boxes are quantum and get random inputs s_A, s_B, you cannot win this game with probability greater than $\cos^2(\pi/8)$. This probability is tight.

$$\frac{1}{4} \sum_{s_A, s_B \in \{0,1\}} \Pr[r_A \oplus r_B = s_A \cdot s_B | (s_A, s_B)] \leq \cos^2(\pi/8)$$

On the other hand, if the boxes are classical, one can win this game with probability at most 3/4.

7.2.2 The protocol

The idea of the protocol is the following. Alice and Bob want to use the GHZ paradox to perform bit commitment. Since only a quantum state can satisfy the GHZ paradox perfectly, they want to use such a state to perform quantum bit commitment as in the non-device independent way. The protocol runs as follows.

Device independent quantum coin flipping

Alice has a box, A, and Bob has a pair of boxes, B and C. The three boxes are supposed to satisfy the GHZ paradox.

- *Commit phase*: Alice inputs into her box the value of the bit she wishes to commit to. Denote the input and output of her box by s_A and r_A. s_A is the bit she commits to. She then selects a classical bit a uniformly at random and sends $c = r_A \oplus (a \cdot s_A)$ as her commitment.
- *Reveal phase*: Alice sends to Bob a, s_A, r_A. Bob first checks if $c = r_A \oplus a \cdot s_A$. He then randomly chooses a pair of inputs s_B and s_C, satisfying $s_A \oplus s_B \oplus s_C = 1$, inputs them into his two boxes B, C. He gets outcomes r_B, r_C and checks that the GHZ paradox is satisfied *i.e.* $r_A \oplus r_B \oplus r_C = s_A s_B s_C \oplus 1$.

If any of these tests fails then he aborts.

Completeness If the parties are honest (and the boxes satisfy the GHZ paradox), then the protocol never aborts.

Alice's cheating probability We consider the worst-case scenario, wherein (dishonest) Alice prepares (honest) Bob's boxes in any state she wants, possibly entangled with her own ancillary systems. Since the commit phase consists of Alice sending a classical bit c as a token of her commitment, without receiving any information from Bob, without loss of generality we may assume that Alice decides on the value of c beforehand, and accordingly prepares Bob's boxes to maximize her cheating probability.

Let us then suppose that Alice sends $c = 0$. A similar analysis can be done if $c = 1$. If Alice wants to reveal $s_A = 0$, she has to reveal $r_A = 0$ (or else the test that $c = r_A \oplus (a \cdot s_A)$ will fail). If Alice wants to reveal $s_A = 1$, she can choose between $r_A = 0$ and $r_A = 1$ (by choosing a accordingly).

Let r_A^1 the value Alice reveals for r_A in case she wants to reveal $s_A = 1$. Since the choice of r_A is fully determined when Alice wants to reveal $s_A = 0$, Alice can also decide the value of r_A^1 beforehand.

- If Alice wants to reveal $s_A = 0$. She sends $r_A = 0$. Bob's second check is only on the boxes B, C. He picks random s_B, s_C with $s_B \oplus s_C = 1$ and checks that $r_B \oplus r_C = s_B \cdot s_C \oplus 1$. In this case,
  $\Pr[\text{Alice successfully reveals } s_A = 0] =$
  $$\frac{1}{2}\left(\Pr[r_B \oplus r_C = 1 | (s_B, s_C) = (0,1)] + \Pr[r_B \oplus r_C = 1 | (s_B, s_C) = (1,0)]\right)$$
- If Alice wants to reveal $s_A = 1$, she sends $r_A = r_A^1$. Bob will then choose random s_B, s_C satisfying $s_B \oplus s_C = 1$ and check that $r_A \oplus r_B \oplus r_C = s_B \cdot s_C \oplus 1$. We have $\Pr[\text{Alice successfully reveals } s_A = 1] =$
  $$\frac{1}{2}\left(\Pr[r_B \oplus r_C = 1 \oplus r_A^1 | (s_B, s_C) = (0,0)] + \Pr[r_B \oplus r_C = r_A^1 | (s_B, s_C) = (1,1)]\right)$$

Let us put everything together. If $r_A^1 = 0$, we have

$$P_A^* = \frac{1}{4} \sum_{s_B, s_C \in \{0,1\}} \Pr[r_B \oplus r_C = s_B \cdot s_C \oplus 1 | (s_B, s_C)]$$

This can be easily reduced to the $CHSH$ inequality as follows. Suppose that the output of the box B is $r'_B = 1 \oplus r_B$. We have

$$P_A^* = \frac{1}{4} \sum_{s_B, s_C \in \{0,1\}} \Pr[r'_B \oplus r_C = s_B \cdot s_C | (s_B, s_C)]$$

which is exactly the CHSH inequality. Note that we can use the CHSH inequality since Bob's two boxes B and C do not communicate. If $r_A^1 = 1$, we use a similar argument to reduce Alice's cheating probability to a CHSH inequality. We conclude that $P_A^* \leq \cos^2(\pi/8)$.

Bob's cheating probability

Bob's most general strategy consists of sending Alice a box entangled with some ancillary system in his possession. Depending on the value of c he receives from Alice (which is uniformly random since Alice is honest), Bob carries out one of a pair of two-outcome measurements on his system. We denote Bob's binary input and output by m_B and g_B, where $m_B = 0$ ($m_B = 1$) corresponds to the measurement he carries out when Alice sends $c = 0$ ($c = 1$), and $g_B = 0$ ($g_B = 1$) corresponds to his guessing that Alice has committed to 0 (1).

We interpret this as follows: honest Alice has a box in which she inputs s_A and outputs r_A. Bob also has some big apparatus where he inputs $m_B = r_A \oplus a \cdot s_A$. His goal is to output $g_B = s_A$. We define $\Pr[x, y|u, v]$ as:

$$\Pr[x, y|u, v] = \Pr[r_A = x, g_B = y | s_A = u, m_B = v]$$

Since a is a random bit, we have

$$P_B^* = \frac{1}{2} \sum_{a,x,y \in \{0,1\}} Pr[s_A = y, m_B = x \oplus (a \cdot y)] \cdot \Pr[x, y|y, (x \oplus (a \cdot y))]$$

We always have $m_B = r_A \oplus a \cdot s_A$ and s_A is a random bit hence

$$\begin{aligned}
P_B^* &= \frac{1}{4} \sum_{a,x,y} \Pr[x, y|y, (x + a \cdot y)] \\
&= \frac{1}{4} \left(\sum_{x,y} \Pr[x, y|y, x] + \sum_{x,y} \Pr[x, y|y, (x \oplus y)] \right) \\
&= \frac{1}{4} (2 \Pr[0, 0|0, 0] + \Pr[0, 1|1, 0] + 2 \Pr[1, 0|0, 1] + \Pr[1, 1|1, 1] + \Pr[0, 1|1, 1] + \Pr[1, 1|1, 0]) \\
&= \frac{1}{4} (X + Y + Z)
\end{aligned}$$

where $X = \Pr[0, 0|0, 0] + \Pr[0, 1|1, 0] + \Pr[1, 1|1, 0]$; $Y = \Pr[1, 0|0, 1] + \Pr[1, 1|1, 1] + \Pr[0, 1|1, 1]$; $Z = \Pr[0, 0|0, 0] + \Pr[1, 0|0, 1]$.

For this proof, we will not use the general device independent condition. We will actually just use the fact that the boxes do not communicate (the

no-signaling condition). For cheating Bob, the security is guaranteed without assuming correctness of our quantum computing model.

The non-signaling condition states the following (see for example [BLM+05])

$$\Pr[r_A = x | s_A = u] = \sum_{y \in \{0,1\}} \Pr[r_A = x, g_B = y | s_A = u, m_B = v] \quad \text{for any } v$$

$$\Pr[g_B = y | m_B = v] = \sum_{x \in \{0,1\}} \Pr[r_A = x, g_B = y | s_A = u, m_B = v] \quad \text{for any } u$$

From these non-signalling condition, we have:

$$\begin{aligned} X &= \Pr[0,0|0,0] + \Pr[0,1|1,0] + \Pr[1,1|1,0] \\ &\leq \Pr[0,0|0,0] + \Pr[1,0|0,0] + \Pr[0,1|1,0] + \Pr[1,1|1,0] \\ &\leq \Pr[g_B = 0 | m_B = 0] + \Pr[g_B = 1 | m_B = 0] \leq 1 \end{aligned}$$

$$\begin{aligned} Y &= \Pr[1,0|0,1] + \Pr[1,1|1,1] + \Pr[0,1|1,1] \\ &\leq \Pr[1,0|0,1] + \Pr[0,0|0,1] + \Pr[1,1|1,1] + \Pr[0,1|1,1] \\ &\leq \Pr[g_B = 0 | m_B = 1] + \Pr[g_B = 1 | m_B = 1] \leq 1 \end{aligned}$$

$$\begin{aligned} Z &= \Pr[0,0|0,0] + \Pr[1,0|0,1] \\ &\leq \Pr[0,0|0,0] + \Pr[0,1|0,0] + \Pr[1,0|0,1] + \Pr[1,1|0,1] \\ &\leq \Pr[r_A = 0 | s_A = 0] + \Pr[r_A = 1 | s_A = 0] \leq 1 \end{aligned}$$

This allows us to conclude that

$$P_B^* = \frac{1}{4}(X + Y + Z) \leq 3/4$$

7.3 Device independent quantum coin flipping

We extend our bit commitment protocol to a coin flipping protocol. We can easily create a bit commitment coin flipping protocol (see Section 4.1.2) with cheating probability $P_A^* = \cos^2(\pi/8)$ and $P_B^* = 3/4$. We will now try to equalize these cheating probabilties.

There is no elegant way to equalize these probabilities. We will consider the simplest way where we use several instances of the device independent coin flipping sequentially. Consider our coin flipping protocol S. Consider now the following Protocol

Two fold repetition of S

- Alice and Bob flip a coin using S.
- If the outcome is 0, they run S again and the outcome becomes the outcome of the protocol. If the outcome is 1, they also run S but now, Alice and Bob exchange behaviors (Alice becomes Bob and Bob becomes Alice)

It is easy to see that Alice's optimal strategy is to try to enforce 0 in the first coin flipping to remain Alice in the second one. She wins with probability $\cos^4\left(\frac{\pi}{8}\right) + \left(1 - \cos^2\left(\frac{\pi}{8}\right)\right) \cdot \frac{3}{4} \simeq 0.838$. On the other hand, Bob wants outcome 1 for the first coin flip and he can win with probability $\frac{3}{4}\cos^2\left(\frac{\pi}{8}\right) + \frac{1}{4} \cdot \frac{3}{4} \simeq 0.827$

Notice that this analysis work because we consider sequential repetition of these protocols. Alice and Bob perform the first coin flip, they get a classical outcome c and then perform the second coin flip. The security of our coin flipping protocol guarantees that during this second coin flip Alice (resp. Bob) has cheating probability at most P_A^* (resp. P_B^*) independently of the outcome of the first coin.

By repeating this procedure, we manage to equalize the probabilities P_A^* and P_B^* and we obtain a device independent coin flipping protocol with cheating probailities equal to 0.836.

7.4 Conclusion

By introducing explicit device independent bit commitment and coin flipping protocols, we have shown that two-party cryptographic primitives can be constructed in the device independent setting. The connection between quantum nonlocality and cryptography, first noted by Ekert twenty years ago [Eke91], is thus seen to apply also in the very rich field of cryptography with mutually distrustful parties (and devices), giving us a new perspective on the connection between cryptography and the foundations of quantum mechanics.

The security guaranteed by our device independent protocols is reasonably close to (though of course greater than) that of the best known device dependent protocols. For the bit commitment protocol we have $P_A^* \simeq 0.854$ and $P_B^* = \frac{3}{4}$, as compared to $P_A^*, P_B^* \lesssim 0.739$ for the optimal device dependent protocol. The coin flipping protocol has a cheating probability of 0.836, as compared to $\frac{1}{\sqrt{2}} \approx 0.707$ in the device dependent case.

It is an open question whether there exists a quantum bit commitment protocol that is secure against dishonest parties limited only by the no-signaling principle, as is the case in quantum key distribution [BHK05, Mas09].

Chapter 8

Loss-tolerant quantum coin flipping and quantum bit commitment

8.1 The loss tolerant model

We now study a different model where we are interested in a specific flaw in the measurement devices: losses. Sometimes, a measurement device will not give any outcome when a measurement is performed. However, when the device gives an outcome, we know that it is the correct outcome. This condition is weaker than the device independent model where we deal with any kind of flaws in the apparatus.

We also add another requirement, that the honest players do not use quantum memory. This requirement did not appear in the previous model. This model is hence incomparable with the device independent model.

In 2008, Berlin *et al.* presented a loss-tolerant quantum coin flipping with a cheating probability of 0.9. In this protocol, honest players do not always succeed when they perform a measurement (the measurement sometimes abort) but when they do succeed, they always output the correct value. This is in contrast with noise tolerance where an honest player could perform a measure with a wrong outcome without knowing it. Recently, Aharon *et al.* [AMS10] created a loss-tolerant quantum coin flipping protocol with a cheating probability of 0.8975. In another flavor, Barrett and Massar [BM04] showed how to do bit-string generation (a weaker notion of coin flipping) in the presence of noise.

In this Chapter, we continue the study of loss-tolerant quantum coin flipping protocol. We construct such a protocol with a cheating probability of 0.859. To achieve this bias, we extend Berlin *et al.* 's protocol by adding an encryption step that hides some information to Bob as long as he does not confirm that he successfully measured. Notice that we improve the bias of the protocol by adding only a classical layer on top of Berlin *et al.* 's protocol.

8.2 The loss-tolerant protocol

8.2.1 The loss-tolerant model

In the loss-tolerant model, we have the following constraints:

1. The measurement devices of honest players have losses. This means when performing a measurement, an honest player can also have an outcome $\perp$ which corresponds to no outcome. In this case, the state is destroyed. However, if the measurement does not yield the $\perp$ then it behaves as a perfect measurement. Especially, there are no errors in the measurement.
2. Honest players should be able to perform the protocol without the use of quantum memory.

8.2.2 Quantum states used

Consider the two orthonormal basis $\mathcal{B}^0(\lambda) = \{|\phi_0^0(\lambda)\rangle, |\phi_1^0(\lambda)\rangle\}$ and $\mathcal{B}^1(\lambda) = \{|\phi_0^1(\lambda)\rangle, |\phi_1^1(\lambda)\rangle\}$ for any $\lambda \in \mathbb{R}$ with:

$$\begin{aligned} |\phi_0^0(\lambda)\rangle &= \sqrt{\lambda}|0\rangle + \sqrt{1-\lambda}|1\rangle \\ |\phi_1^0(\lambda)\rangle &= \sqrt{1-\lambda}|0\rangle - \sqrt{\lambda}|1\rangle \end{aligned}$$

and

$$\begin{aligned} |\phi_0^1(\lambda)\rangle &= \sqrt{\lambda}|0\rangle - \sqrt{1-\lambda}|1\rangle \\ |\phi_1^1(\lambda)\rangle &= \sqrt{1-\lambda}|0\rangle + \sqrt{\lambda}|1\rangle \end{aligned}$$

$|\phi_c^b\rangle$ corresponds to the encoding of bit c in basis b.
Finally, we define

$$\rho_c = \frac{1}{2}\sum_i |\phi_c^i\rangle\langle\phi_c^i| = \lambda|c\rangle\langle c| + (1-\lambda)|1-c\rangle\langle 1-c|$$

8.2.3 Berlin *et al.* 's protocol for quantum coin flipping

Berlin *et al.* 's protocol (parameter λ omitted)

1. Alice chooses at random $b \in_R \{0,1\}$ and $c \in_R \{0,1\}$ and sends $|\phi_c^b\rangle$ to Bob.
2. Bob chooses $b' \in_R \{0,1\}$ and measures the qubit he receives in basis $B_{b'}$. If his measurement fails, he announces it to Alice and they repeat the protocol from step 1. If the measurement succeeds continue.
3. Bob picks $c' \in_R \{0,1\}$ and sends c' to Alice
4. Alice reveals b, c
5. If $b = b'$, Bob checks that what he measured corresponds to $|\phi_c^b\rangle$. If it does not match, he aborts.
6. The outcome of the protocol is $x = c \oplus c'$.

This protocol is loss tolerant in the sense that a cheating Bob cannot gain advantage from the fact that he can restart the protocol when his measurement fails. This protocol has the following security parameters:

- $P_A^* = \frac{1}{2} + \frac{1+\mathrm{F}(\rho_0,\rho_1)}{4} = \frac{3}{4} + \frac{\sqrt{\lambda(1-\lambda)}}{2}$
- $P_B^* = \frac{1+\Delta(\rho_0,\rho_1)}{2} = \lambda$

By taking $\lambda = 0.9$, we have $P_A^* = P_B^* = 0.9$.

This protocol is a bit-commitment based protocol and is very similar to the protocols described in Section 4.1.2. The only difference is that Bob measures directly the state he receives in order to satisfy requirement 2. (no quantum memory) of the loss-tolerant model. Berlin *et al.* showed that Bob's lossy detectors do not decrease security of the protocol. If we did not require the absence of quantum memory, we would have $P_A^* = \frac{1+\mathrm{F}(\rho_0,\rho_1)}{2}$

8.2.4 Our protocol

Our protocol

1. Alice chooses at random $b_1, b_2 \in_R \{0,1\}$; $c \in_R \{0,1\}$ and $r_1, r_2 \in_R \{0,1\}$ sends two quantum registers $|\phi^{b_i}_{c\oplus r_i}\rangle$ for $i \in \{1,2\}$ to Bob.
2. Bob chooses $b'_1, b'_2 \in_R \{0,1\}$ and measures each register i he receives in basis $B_{b'_i}$. If one of his measurements fails, he announces it to Alice and they repeat the protocol from step 1. If the measurement succeeds, Bob announces this fact to Alice and they continue.
3. Alice sends r_1, r_2 to Bob.
4. Bob picks $c' \in_R \{0,1\}$ and sends c' to Alice
5. Alice reveals b_1, b_2, c
6. For each register i for which $b_i = b'_i$, Bob checks that what he measured corresponds to $|\phi^{b_i}_{c\oplus r_i}\rangle$. If one of the measurements does not match, he aborts.
7. The outcome of the protocol is $x = c \oplus c'$.

This protocol is closely related to a two-fold parallel repetition of Berlin *etal*'s protocol. Such a repetition would directly improve the bias if we did not require loss tolerance. We add an additional step in this protocol. Alice hides some information about the state she sends using 2 private bits r_1, r_2 that she reveals as soon as Bob confirms that he measured successfully. As we will show, this makes the protocol loss-tolerant again.

8.3 Security proofs

If Alice and Bob are honest then Bob never aborts and $x = c \oplus c'$ is random. We now analyse separately cheating Alice and cheating Bob.

8.3.1 Cheating Alice

We consider a cheating Alice and an honest Bob.

General framework for a checking Bob

The way Bob checks is closely related to the following procedure

- Alice sends a state σ in space $\mathcal{Y}$
- At a later stage, Alice sends a bit i to Bob in space $\mathcal{X}$
- Bob checks that the first state Alice sends in $\mathcal{Y}$ is the state $|\psi_i\rangle$ for some state $|\phi_i\rangle$.

We extend the notion of fidelity for ensembles of quantum states.

Definition 15 *Let E and F any two ensembles of quantum states and let ρ any quantum state. We define:*

$$\begin{aligned} F(\rho, E) &= \max_{\sigma \in E} F(\rho, \sigma) \\ F(E, F) &= \max_{\sigma \in E, \sigma' \in F} F(\sigma, \sigma') \end{aligned}$$

We want to show the following:

Proposition 20

$$\Pr[\ \textit{Alice passes Bob's test}\ ] \leq F^2(\sigma, L)$$

where $L = \{\sum_j p_i |\phi_j\rangle\langle\phi_j| : \ \sum_j p_j = 1\}$

Proof: Let σ the first state in $\mathcal{Y}$ sent by Alice and let $\widetilde{\sigma}$ the state in $\mathcal{X}\mathcal{Y}$ after Alice reveals i. Since Bob immediately measures the register $\mathcal{X}$ in the computational basis, there is an state $\widetilde{\sigma}$ which will give the best cheating probability of the form $\widetilde{\sigma} = \sum_i p_i |i\rangle\langle i| \otimes |\psi_i\rangle\langle\psi_i|$ and

$$\Pr[\ \text{Alice passes Bob's test}\ ] = \sum_i |\langle\psi_i|\phi_i\rangle|^2$$

Similarly, if we fix $\widetilde{\sigma} = |\Omega\rangle\langle\Omega|$ where $|\Omega\rangle = \sum_i \sqrt{p_i}|i, \phi_i\rangle$, we get that Pr[Alice passes Bob's test] = $\sum_i ||\psi_i\rangle\langle\phi_i||^2$ This means that we can suppose wlog that after the last step, the state in $\mathcal{X}\mathcal{Y}$ is pure.

Let $\widetilde{\sigma} = |\Omega\rangle\langle\Omega|$ where $|\Omega\rangle = \sum_i \sqrt{p_i}|i, \phi_i\rangle$. Let K subspace of quantum pure states spanned by $\{|i\rangle \otimes |\phi_i\rangle\}$. Let $P_K = \sum_i |i\rangle\langle i| \otimes |\phi_i\rangle\langle\phi_i|$ the projection on

subspace K. Bob's check is equivalent to projecting on the subspace K.

$$\begin{aligned}
\Pr[\text{ Alice passes Bob's test }] &= tr(P_K \widetilde{\sigma} P_K) \\
&= tr(P_K |\Omega\rangle\langle\Omega| P_K) = \max_{|u\rangle \in L} |\langle\Omega|u\rangle|^2 \\
&\leq \max_{|u\rangle \in K} F^2(\mathrm{Tr}_{\mathcal{X}}(|\Omega\rangle\langle\Omega|), \mathrm{Tr}_{\mathcal{X}}|u\rangle\langle u|) \\
&\leq \max_{|u\rangle \in K} F^2(\sigma, \mathrm{Tr}_{\mathcal{X}}|u\rangle\langle u|) \\
&\leq F^2(\sigma, L) \quad \text{since } \forall |u\rangle \in K,\ \mathrm{Tr}_{\mathcal{X}}|u\rangle\langle u| \in L
\end{aligned}$$

■

Proof of security for cheating Alice

We consider a cheating Alice and an honest Bob. For the sake of the analysis, we can suppose that honest Bob does not have losses when he measures (this does not help Alice). Our protocol says that Bob measures each register i in a random basis $B_{b'_i}$ and performs a check if this basis corresponds to the basis B_{b_i} in which Alice encoded c. Similarly, we could say that Bob performs this measurement at the very end (still picking b'_i at random). In this case, we are in the framework of the previous subsection except that with some probability, Bob chooses the wrong basis and does not check anything.

Suppose Alice wants to reveal c in our protocol. Let ξ the state in $\mathcal{XY}$ she sends at stage 1. Let $\xi_X = \mathrm{Tr}_{\mathcal{Y}}\xi$ and $\xi_Y = \mathrm{Tr}_{\mathcal{X}}\xi$. Let $L_c = \{\sum_{i\in\{0,1\}} p_i |\phi^i_c\rangle\langle\phi^i_c|\}$

We have the following cases:

- Bob flipped $b'_1 \neq b_1$ and $b'_2 \neq b_2$. Bob does not check anything Alice successfully reveals c with probability 1.
- Bob flipped $b'_1 = b_1$ and $b'_2 \neq b_2$. Bob checks the first register. From Proposition 20, Alice successfully reveals c with probability no greater than $F^2(\xi_X, L_c)$.
- Bob flipped $b'_1 \neq b_1$ and $b'_2 = b_2$. Bob checks the second register. Similarly, Alice successfully reveals c with probability no greater than $F^2(\xi_Y, L_c)$.
- Bob flipped $b'_1 = b_1$ and $b'_2 = b_2$. Bob checks both registers. In the same way, Alice successfully reveals c with probability no greater than $F^2(\xi, L_c^{\otimes 2})$.

This gives us

$$\Pr[\text{ Alice successfully reveals } c] = \frac{1}{4}\left(1 + F^2(\xi_X, L_c) + F^2(\xi_Y, L_c) + F^2(\xi, L_c \otimes 2)\right)$$

We will now need the following Lemma

Lemma 6

$$F(L_0, L_1) \leq 2\sqrt{\lambda(1-\lambda)}$$

Proof: Let $\rho_0 \in L_0$ and $\rho_1 \in L_1$ such that $F(\rho_0, \rho_1) = F(L_0, L_1)$. By definition of L_0, we have $\langle 0|\rho_0|0\rangle = \lambda$ and $\langle 0|\rho_1|0\rangle = 1 - \lambda$. This gives us $\Delta(\rho_0, \rho_1) \geq 2\lambda - 1$. Using the Proposition 9 (Section 3.6), we have

$$\begin{aligned} F(\rho_0, \rho_1) &\leq \sqrt{1 - \Delta^2(\rho_0, \rho_1)} \\ &\leq \sqrt{1 - 4\lambda^2 + 4\lambda - 1} \\ &\leq 2\sqrt{\lambda(1-\lambda)} \end{aligned}$$

■

We can now prove our main statement

Proposition 21

$$P_A^* \leq \frac{1}{2} + \frac{1}{2}\left(\frac{1 + f(\lambda)}{2}\right)^2$$

where $f(\lambda) = 2\sqrt{\lambda(1-\lambda)}$

Proof: We suppose w.log that Alice wants final outcome $x = 0$. This means that she has to reveal $c = c'$. Let ξ the state sent by Alice and let $\xi_X = \mathrm{Tr}_{\mathcal{Y}}\xi$ and $\xi_X = \mathrm{Tr}_{\mathcal{Y}}\xi$. Since c' is random, we have

$$\begin{aligned} P_A^* &= \frac{1}{2}\sum_{c\in\{0,1\}} \Pr[\text{ Alice successfully reveals } c] \\ &\leq \sum_{c\in\{0,1\}} \frac{1}{4}\left(1 + F^2(\xi_X, D_c) + F^2(\xi_Y, D_c) + F^2(\xi, DD_c)\right) \\ &\leq \frac{1}{8}\left(2 + 1 + F(D_0, D_1) + 1 + F(D_0, D_1) + 1 + F(DD_0, DD_1)\right) \quad (\textit{Proposition } 8) \\ &\leq \frac{1}{2} + \frac{1}{2}\left(\frac{1}{4} + \frac{1}{2}F(D_0, D_1) + \frac{1}{4}F^2(D_0, D_1)\right) \\ &\leq \frac{1}{2} + \frac{1}{2}\left(\frac{1 + f(\lambda)}{2}\right)^2 \quad (f(\lambda) \geq F(D_0, D_1) \text{ from Lemma 6}) \end{aligned}$$

■

8.3.2 Cheating Bob

The main part here is to show the loss-tolerance of the protocol. This means that a cheating Bob cannot take advantage of the fact that he's allowed to reset the protocol in case one of his measurements failed.

Loss tolerance For a fixed c and r_1, r_2, let $\xi_c^{r_1,r_2}$ sent by Alice. We have

$$\begin{aligned} \xi_c^{r_1,r_2} &= \frac{1}{4}\sum_{b_1,b_2\in\{0,1\}} |\phi_{c\oplus r_1}^{b_1}\phi_{c\oplus r_2}^{b_2}\rangle\langle\phi_{c\oplus r_1}^{b_1}\phi_{c\oplus r_2}^{b_2}| \\ &= \rho_{c\oplus r_1} \otimes \rho_{c\oplus r_2} \\ &= \sum_{u,v\in\{0,1\}} p_{c\oplus r_1, c\oplus r_2}^{u,v} |u,v\rangle\langle u,v| \end{aligned}$$

where: if $x = y$ then $p_x^y = \lambda$; if $x \neq y$ then $p_x^y = 1 - \lambda$ and $p^{u,v}_{c\oplus r_1, c\oplus r_2} = p^u_{c\oplus r_1} \cdot p^v_{c\oplus r_2}$.

When receiving ξ, Bob performs a quantum operation

$$A(|u,v\rangle) = \alpha_{u,v}|\psi_{u,v}\rangle|0\rangle_{\mathcal{O}} + \beta_{u,v}|\omega_{u,v}\rangle|1\rangle_{\mathcal{O}}$$

where $\mathcal{O}$ is the space that Bob measures to determine whether he should announce that he measured successfully or not. The outcome 0 in space $\mathcal{O}$ corresponds to the outcome where the protocol continues. In a way, the cheating Bob postselects on the outcome being 0 since if he obtains 1, he decides to start the protocol again. Once Bob successfully measured and after Alice sends r_1, r_2, Bob has the following state depending on the operation A he performed averaging on r_1, r_2.

$$\xi_c^A = \frac{1}{S} \sum_{\substack{r_1,r_2\in\{0,1\}\\ u,v\in\{0,1\}}} p^{u,v}_{c\oplus r_1, c\oplus r_2} \Gamma_{u,v} |r_1, r_2, \psi_{u,v}\rangle\langle r_1, r_2, \psi_{u,v}|$$

where

- The $\Gamma_{u,v}$'s are arbitrary real numbers. These numbers depend on the $\alpha_{u,v}$'s. We assume that Bob can choose any value for these numbers.
- The $|\psi_{u,v}\rangle$'s are not necessarily orthogonal.
- S is a normalization factor.

Proposition 22 *$\forall A$, $\Delta(\xi_0^A, \xi_1^A) \leq \Delta(\xi_0, \xi_1)$ where $\xi_c = \rho_c^{\otimes 2}$.*

Proof: Let's fix A. From the definition of ξ_c^A and from Proposition 4, we have

$$\begin{aligned}
\Delta(\xi_0^A, \xi_1^A) &\leq \frac{1}{2S} \sum_{\substack{r_1,r_2\in\{0,1\}\\ u,v\in\{0,1\}}} |p^{u,v}_{r_1,r_2}\Gamma_{u,v} - p^{u,v}_{1\oplus r_1, 1\oplus r_2}\Gamma_{u,v}| \\
&\leq \frac{1}{2S} \sum_{u,v} \Gamma_{u,v} \sum_{r_1,r_2} |p^{u,v}_{r_1,r_2} - p^{u,v}_{1\oplus r_1, 1\oplus r_2}|
\end{aligned}$$

To calculate this sum, if $(r_1, r_2) = (u, v)$ then $p^{u,v}_{r_1,r_2} = \lambda^2$ and $p^{u,v}_{1\oplus r_1, 1\oplus r_2} = (1-\lambda)^2$. If $(r_1, r_2) = (\overline{u}, \overline{v})$ then $p^{u,v}_{r_1,r_2} = (1-\lambda)^2$ and $p^{u,v}_{1\oplus r_1, 1\oplus r_2} = \lambda^2$. In the other cases, $p^{u,v}_{r_1,r_2} = p^{u,v}_{1\oplus r_1, 1\oplus r_2}$. This gives us

$$\begin{aligned}
\Delta(\xi_0^A, \xi_1^A) &\leq \frac{1}{2S} \sum_{u,v} 2\Gamma_{u,v} \left(\lambda^2 - (1-\lambda)^2\right) \\
&\leq 2\lambda - 1
\end{aligned}$$

Since, $\xi_c = \lambda^2 |cc\rangle\langle cc| + \lambda(1-\lambda)(|01\rangle\langle 01| + |10\rangle\langle 10|) + (1-\lambda)^2 |\overline{c}\ \overline{c}\rangle\langle \overline{c}\ \overline{c}|$, we have $\Delta(\xi_0, \xi_1) = (\lambda^2 - (1-\lambda)^2) = 2\lambda - 1$, which allows us to conclude. ■

We can now prove our main Claim

Proposition 23 $P_B^* \leq \lambda$

Proof: Suppose w.log that Bob wants outcome $x = 0$. He wants to pick $c' = c$. Before picking c', he has the state ξ_c^A. We have

$$\begin{aligned} P_B^* &= \Pr[\text{ Bob guesses } c] \\ &= \frac{1}{2} + \frac{\Delta(\xi_0^A, \xi_1^A)}{2} \\ &\leq \lambda \end{aligned}$$

■

Theorem 10 *There is a loss-tolerant quantum coin flipping protocol with bias* $\varepsilon \approx 0.359$.

Proof: We just need to find λ that minimizes $\max(P_A^*, P_B^*)$. The maximum is achieved for $\lambda \approx 0.859$ which gives $P_A^* = P_B^* \approx 0.859$ which gives a bias $\varepsilon \approx 0.359$. ■

8.4 Further discussion

Optimality of the bias The bias that we show here is actually not optimal for the protocol. The reason is the following: in the analysis of cheating Alice (Section 8.3.1), we consider the cheating probability for Alice depending on whether Bob checks the first bit, the second bit or both bits. For each of these cases, we upper bound Alice's cheating probability. But it appears that the cheating probabilities for each of these cases is different and that Alice cannot cheat optimally for all these cases at the same time. This slightly decreases Alice's cheating probability. We can numerically calculate in this case that for $\lambda \approx 0.858$, we have $P_A^* = P_B^* \approx 0.858$. This gives a bias of $\varepsilon \approx 0.858$ which is a slight improvement over what is shown.

Multiple repetition Our protocol consists of a two-fold repetition of Berlin *et al.* 's protocol. What happens if we consider a k-fold repetition? Even if it is difficult to calculate the exact cheating probabilities of Alice and Bob in the case of multiple repetitions, these probabilities can be easily upper and lower bounded. We use the following bounds. Let $P_A^*(k, \lambda)$ the cheating probability for Alice (resp. Bob) with a k-fold repetition of Berlin *et al.* 's protocol with parameter λ. Let $P(k) = \min_\lambda(\max\{P_A^*(k, \lambda), P_B^*(k, \lambda)\})$. $P(k)$ corresponds to the best cheating probability when considering a k-fold repetition of the protocol. We need to lower bound $P_A^*(k, \lambda)$. We have

$$P_A^*(k, \lambda) \leq f(k, \lambda) = \frac{1}{2} + \frac{1}{2}\left(\frac{1}{2} + \sqrt{\lambda(1-\lambda)}\right)^k$$

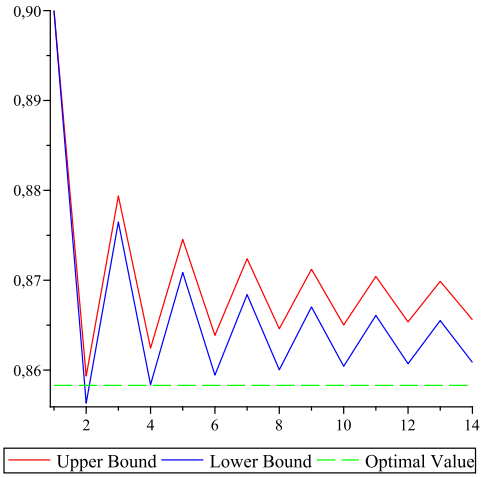
This is a generalization of the upper bound we use to show that $\varepsilon \approx 0.359$. Intuitively, this corresponds to the case where Alice knows if Bob measured in the correct basis or not. When we consider Alice's cheating strategies where she uses separate (non entangled) strategies for each of the k repetitions, we have the following lower bound.

$$P_A^*(k, \lambda) \geq g(k, \lambda) = (\frac{3}{4} + \frac{\sqrt{\lambda(1-\lambda)}}{2})^k$$

On the other hand, it is possible to calculate exactly Bob's cheating probability since

$$P_B^*(k,\lambda) = 1/2 + \Delta(\rho_0^{\otimes k}, \rho_1^{\otimes k})/2$$

Using these bounds, we get the following diagram for cheating probabilities of Alice and Bob which shows that the optimal value is achieved using a 2-fold repetition of the protocol. The x-axis corresponds to the number of repetition k. The y-axis corresponds to the minimal cheating probability $P(k)$ when using lower/upper bounds for P_A^*.



Chapter 9

Relationship between quantum zero-knowledge proofs and quantum bit commitment

9.1 Introduction

In this Chapter, we go beyond the scope of information theoretic security and study quantum computational bit commitment schemes. We study complexity assumptions that imply such commitment schemes. We will show that the existence of quantum computationally secure bit commitments is closely related to quantum zero-knowledge classes and quantum interactive proofs.

9.1.1 Zero-knowledge proofs

One of the main goals of modern cryptography is to give a formal and practical way of defining security for given protocols. Some theoretically secure objects such as one-way functions have been defined. Assuming the hardness of certain problems, we can create these secure objects and therefore prove that a given protocol is secure. One can also base security on information-theoretic based arguments. These arguments are much stronger because they do not rely on any computational assumption but are usually much harder to achieve.

It's in this setting that Zero-Knowledge proofs were invented. Consider a problem P that is believed hard. Suppose that one person (the Prover) can prove to another person (the Verifier) that the answer to the problem is YES without giving any other information. In particular, the Verifier will not be able to convince someone else that the answer to this problem is YES. In order to create this kind of proofs, the Prover and the Verifier must interact with each other. The condition "Without giving any other information" has been formalized in a simple and elegant way by [GMR89] and this security condition has been defined in the computational setting as well as the information-theoretical setting. The true power of Zero-Knowledge started to be understood in [GMW91] where it

was shown that all of NP has computational Zero-Knowledge proofs.

To get a better understanding of Zero-Knowledge proofs, let's look at an example. Suppose that the prover creates 2 isomorphic graphs G_1 and $G_2 = \sigma_0(G_1)$. He wants to convince the verifier that these 2 graphs are isomorphic but without giving him any information. In particular, the verifier will have no information about σ_0. Note that the graph isomorphism problem is believed to be a hard and a polynomial time verifier is not able to determine by himself if the 2 graphs are isomorphic or not. Consider the following protocol :

Zero-Knowledge protocol for the Graph Isomorphism problem

P : Choose a random permutation σ and send $G' = \sigma(G_1)$ to the verifier.

V : Choose at random $b \in \{1, 2\}$ and send it to the verifier

P : Send σ' to the verifier such that $\sigma'(G') = G_b$.

Without going into deep analysis of this protocol, note the following :

- If the graphs are isomorphic then the prover will always be able to find a correct σ' and the verifier will always be convinced.
- If the graphs are non-isomorphic then whatever the prover sends to the verifier as a first graph G', he will not be able to find a correct σ' for both $b = 1$ and $b = 2$. His probability of convincing the verifier is therefore $\leq 1/2$. Note that some techniques can reduce this probability to $1/2^k$.
- Suppose the graphs are isomorphic. Let's look what information the verifier has at the end of the protocol. The verifier has a random graph G' isomorphic to G_b and the isomorphism that goes from G' to G_b. He can obtain this information by himself by just by picking a random permutation and apply it to G_b. Therefore, he gains no information. Note that we are interested in keeping the Prover's secret only if the assertion is true. Note also that the verifier cannot gain any information by sending a biased coin.

Classical zero-knowledge proofs have been widely studied [GMR89, BGG$^+$90, Vad99] and especially their relationship with cryptographic primitives such as one-way functions. Ostrovsky and Wigderson [OW93] proved, at a high level, that if Computational Zero Knowledge (ZK) is not trivial then there exists a family of functions that are not 'easy to invert'. The result was extended by Vadhan [Vad06] to show that if ZK does not equal Statistical Zero Knowledge (SZK), then there exists an auxiliary-input one-way function, i.e. one can construct a one-way function given an auxiliary input (or else advice). Looking at auxiliary-input cryptographic primitives is convenient, since we are looking at worst-case complexity classes. Last, Ostrovsky and Wigderson also showed that if ZK contains a 'hard-on-average' problem, then 'regular' one-way functions exist.

9.1.2 Relationship between quantum commitments and quantum zero-knowledge proofs

We study complexity assumptions under which quantum commitment schemes exist. We only look at worst-case complexity classes, and hence similar to the classical case, we obtain auxiliary-input commitments, i.e. commitments that can be constructed with classical and/or quantum advice. Needless to say, since our commitments are quantum, we define the computationally binding and hiding properties against quantum poly-time adversaries (that are also allowed to receive an arbitrary quantum auxiliary input).

We extend these results to the quantum case but we are intersted in quantum bit commitment instead of quantum one-way functions. Our first result, involves the class of Quantum Statistical Zero Knowledge, QSZK, and states the following

Theorem 11 *If* QSZK $\not\subseteq$ QMA *there exists a non-interactive auxiliary-input quantum statistically binding-computationally hiding commitment scheme.*

Before explaining this result, let us try to see what an equivalent classical result would mean. At a high level, the classical statement would be of the following form: if SZK is not in MA, then auxiliary-input commitments exist. However, under some derandomization assumptions, we have that NP = MA = AM ([MV06, KvM02]) and since SZK $\subseteq$ AM, we conclude that SZK $\subseteq$ MA. Hence, the equivalent classical assumption is quite strong and, if one believes in derandomization, possibly false.

However, in the quantum setting, it would be surprising if QSZK is actually contained in QMA. We know that QSZK $\subseteq$ QIP[2] [Wat09], where QIP[2] is the class of languages that have quantum interactive proofs with two messages (note that one only needs three messages to get the whole power of quantum interactive proofs). So far, any attempt to reduce QIP[2] to QMA or find any plausible assumptions that would imply it, have not been fruitful. The main reason is that the verifier's message cannot be reduced to a public coin message nor to a pure quantum state. His message is entangled with his quantum workspace and this seems inherent for the class QIP[2]. It would be striking if one can get rid of this entanglement and reduce the class to a single message from the prover.

Last, if we weaken the security condition to hold against quantum adversaries with only classical auxiliary input, then the above assumption also becomes weaker, i.e. QSZK $\not\subseteq$ QCMA, where QCMA is the class where the quantum verifier receives a single classical message from the prover.

It is not known whether the condition QSZK $\subseteq$ QMA holds. Recently, it Aaronson showed that $\mathsf{HVQSZK}^A \subseteq \mathsf{QMA}^A$ for some oracle A. This means that the inequality holds in some restricted model, and gives some evidence that the inequality holds in general

We then turn our attention to even weaker complexity assumptions about quantum interactive proofs. More precisely, we look at the class QIP (which is believed to be much larger than QSZK) and its relation to QMA and show the following

Theorem 12 *If* QIP $\not\subseteq$ QMA *there exist non-interactive auxiliary-input quantum commitment schemes (both statistically hiding-computationally binding and statistically binding-computationally hiding) with quantum advice.*

Note, that QIP = PSPACE [JJUW10] and QMA $\subseteq$ PP [MW05], so our assumption is extremely weak, in fact weaker than PSPACE $\not\subseteq$ PP. Of course, with such a weak assumption we get a weaker form of commitment: the advice is now quantum (and classical). This means that in order for the prover and the verifier to efficiently perform the commitment for a security parameter n, they need to receive a classical auxiliary input as well as quantum advice of size polynomial in n. This quantum advice is a quantum state on poly(n) qubits that is not efficiently constructible (otherwise, we could have reduced the quantum advice to classical advice by describing the efficient circuit that produces it). Moreover, the quantum advice we consider does not create entanglement between the players.

The key point behind this result is the structure of QIP. More precisely, we use the fact that there exists a QIP-complete problem where the protocol has only three rounds and the verifier's message is a single coin. The equivalent classical result would say that if three-message protocols with a single coin as a second message are more powerful than MA then commitments exist. Again, classically, if we believe that AM = MA, then this assumption is false. Taking this assumption to the quantum realm, it becomes 'almost' true, unless PSPACE = PP.

Let us also note that all our commitments are non-interactive, a feature that could be useful for applications. Last, from the QIP $\not\subseteq$ QMA assumption we construct both statistically hiding-computationally binding commitments and statistically binding-computationally hiding ones, whose constructions are conceptually different. In order to prove the security of the second construction we prove a parallel repetition result for protocols based on the swap test that may be of independent interest. From the QSZK $\not\subseteq$ QMA assumption we show only the construction of statistically binding-computationally hiding commitments, but one can also similarly construct statistically hiding-computationally binding commitments.

9.1.3 Quantum interactive complexity classes

The class QMA, first studied in [Wat00], is informally the class of all problems that can be verified by a quantum polynomial-time verifier with access to a quantum proof.

Definition 16 *A language L is in* QMA *if there is poly-time quantum verifier V such that*

1. *if $x \in L$, then there exists a state ρ such that* $\Pr[V(x,\rho)$ *accepts*$] \geq a$,
2. *if $x \notin L$, then for any state ρ,* $\Pr[V(x,\rho)$ *accepts*$] \leq b$,

where a, b are any efficiently computable functions of $|x|$ such that $|a-b|$ is at least an inverse polynomial [KSV02, MW05].

If in the above definition the witness state ρ is restricted to be a classical witness while keeping a quantum poly-time verifier, then the class is called QCMA.

The class QIP, first studied in [Wat03], consists of those problems that can be interactively verified in quantum polynomial time. A recent result has shown that QIP = PSPACE [JJUW10].

Definition 17 *A language $L \in \mathsf{QIP}$ if there is a polynomial time quantum algorithm V exchanging quantum messages with a computationally unbounded prover P such that, for any input x*

1. *if $x \in L$, then there exists a prover P such that, (V, P) accepts with probability at least a.*
2. *if $x \notin L$, then for any prover P, (V, P) accepts with probability at most b.*

As in the case of QMA*, we need only require that $|a - b|$ is at least an inverse polynomial in the input size [KW00].*

One key property of QIP is that any quantum interactive proof system can be simulated by one using only three messages [KW00]. This is not expected to hold in the classical case, as it would imply that $\mathsf{PSPACE} = \mathsf{AM}$. This property allows us to define simple complete problems involving quantum circuit for the class.

In what follows we consider quantum unitary circuits C, that output a state in the space $\mathcal{O} \otimes \mathcal{G}$. These spaces can be different for each circuit. $\mathcal{O}$ corresponds to the output space and $\mathcal{G}$ to the garbage space. For any circuit C, we define $|\phi_C\rangle = C|0\rangle$ in the space $\mathcal{O} \otimes \mathcal{G}$ to be the output of the circuit before the garbage space is traced out, and $\rho^C = \mathrm{Tr}_{\mathcal{G}}(|\phi_C\rangle\langle\phi_C|)$ to be the mixed state output by the circuit after the garbage space is traced out. We will also consider mixed-state quantum circuits C,that take as input a mixed quantum state σ and output a mixed quantum state, denoted by $C(\sigma)$. Note that circuits of this form can (approximately) represent any quantum channel. The size of a circuit C is equal to the number of gates in the circuit plus the number of qubits used by the circuit. This is denoted $|C|$. We will also use the notation $|\mathcal{X}|$ to refer to the size of a Hilbert space $\mathcal{X}$, which is the number of qubits needed to represent a vector in the space, i.e. $|X| = \lceil \log_2 \dim X \rceil$. We now describe some complete problems for the class.

Definition 18 (QCD Problem) *Let μ a negligible function. We define the promise problem Quantum Circuit Distinguishability* $\mathrm{QCD} = \{\mathrm{QCD}_Y, \mathrm{QCD}_N\}$ *as follows*

- *Input: two mixed-state quantum circuits C_0, C_1 of size n.*
- $(C_0, C_1) \in \mathrm{QCD}_Y \Leftrightarrow \| C_0 - C_1 \|_\diamond \geq 2 - \mu(n)$
- $(C_0, C_1) \in \mathrm{QCD}_N \Leftrightarrow \| C_0 - C_1 \|_\diamond \leq \mu(n)$

Quantum Circuit Distinguishability is QIP-complete [RW05].

9.1.4 A new complete problem for QIP

In this Section, we construct a new problem which is complete for QIP.

Definition 19 (Π Problem) *Let μ a negligible function. We define the following promise problem $\Pi = \{\Pi_Y, \Pi_N\}$:*

- *Input: two mixed-state quantum circuits C_0, C_1 of size n that take as input quantum states in $\mathbf{D}(\mathcal{X} \otimes \mathcal{Y})$ and output a single bit .*

- $(C_0, C_1) \in \Pi_Y \Leftrightarrow \exists \rho^0, \rho^1 \in \mathbf{D}(\mathcal{X} \otimes \mathcal{Y})$ *with* $tr_{\mathcal{X}}(\rho^0) = tr_{\mathcal{X}}(\rho^1)$ *such that*

$$\frac{1}{2}\left(\Pr[C_0(\rho^0) = 1] + \Pr[C_1(\rho^1) = 1]\right) = 1$$

- $(C_0, C_1) \in \Pi_N \Leftrightarrow \forall \rho^0, \rho^1 \in \mathbf{D}(\mathcal{X} \otimes \mathcal{Y})$ *with* $tr_{\mathcal{X}}(\rho^0) = tr_{\mathcal{X}}(\rho^1)$, *we have*

$$\frac{1}{2}\left(\Pr[C_0(\rho^0) = 1] + \Pr[C_1(\rho^1) = 1]\right) \leq \frac{1}{2} + \mu(n)$$

Proposition 24 *The promise problem* Π *problem is also complete for* QIP

Proof: We prove this proposition via a reduction from the Close Images problem, which is complete for QIP [KW00]. This problem can be defined as

Problem 13 (Close Images) *The input to the problem is two mixed-state quantum circuit* Q_0 *and* Q_1 *that implement transformations from* $\mathbf{D}(\mathcal{I})$ *to* $\mathbf{D}(\mathcal{O})$, *where* n *is the number of input qubits to the circuits and* $|(Q_0, Q_1)| \in \text{poly}(n)$. *The promise problem is to distinguish the two cases:*

Yes: $Q_0(\sigma_0) = Q_1(\sigma_1)$ *for some* $\sigma_0, \sigma_1 \in \mathbf{D}(\mathcal{I})$,

No: $\mathrm{F}(Q_0(\sigma_0), Q_1(\sigma_1)) \leq 2^{-n}$ *for all* $\sigma_0, \sigma_1 \in \mathbf{D}(\mathcal{I})$.

Before giving the reduction, we first observe that the problem Π is in QIP. This is done using the following protocol:

Protocol 14 *On input* (C_0, C_1) *an instance of* Π.

1. *P sends the portion of* ρ^0 *that lies in* $\mathcal{Y}$.
2. *V chooses* $i \in \{0, 1\}$ *at random and sends it to P.*
3. *P sends a state in* $\mathcal{X}$ *so that V has the state* ρ^i. *V computes* $C_i(\rho^i)$ *and accepts if and only if the output is 1.*

Note that in Step 3 the honest prover can always send a state in $\mathcal{X}$ so that the verifier holds ρ^i. This follows from the unitary equivalence of all purifications of the state $\mathrm{tr}_{\mathcal{X}} \rho^0 = \mathrm{tr}_{\mathcal{X}} \rho^1$.

Consider the probability that the verifier accepts in Protocol 14. At Step 3 the Verifier holds one of two states ρ^0 and ρ^1 with the property that $\mathrm{tr}_{\mathcal{X}} \rho^0 = \mathrm{tr}_{\mathcal{X}} \rho^1$, because the Prover is forced to commit to the portion of the state in $\mathcal{Y}$ before learning i. Notice also that the Prover can send one of two arbitrary states satisfying the reduced-state property. Since the Verifier runs each of the two circuits with uniform probability, he can be made to accept with probability exactly

$$\frac{1}{2} \max_{\substack{\rho^0, \rho^1 \in \mathbf{D}(\mathcal{X}, \mathcal{Y}) \\ \mathrm{tr}_{\mathcal{X}} \rho^0 = \mathrm{tr}_{\mathcal{X}} \rho^1}} \left(\Pr[C_0(\rho^0) = 1] + \Pr[C_1(\rho^1) = 1]\right).$$

This implies that if $(C_0, C_1) \in \Pi_Y$ then V accepts with probability at least $1 - \mu(n)$, and if $(C_0, C_1) \in \Pi_N$, then V accepts with probability at most $1/2 + \mu(n)$, which puts the problem Π into QIP.

To see that the problem is hard for QIP, let Q_0, Q_1 be the circuits from an instance of the Close Images problem. By the standard technique of moving the

measurements to the end of the circuit, we may assume that these circuits are given as unitary circuits $U_0, U_1 \colon \mathcal{I} \otimes \mathcal{A} \to \mathcal{O} \otimes \mathcal{G}$ such that

$$Q_i(\sigma) = \operatorname{tr}_{\mathcal{G}} U_i(\sigma \otimes |0\rangle\langle 0|)U_i^\dagger,$$

where $\mathcal{A}$ corresponds to the space of any ancillary qubits introduced in the $|0\rangle$ state. From these circuits we construct the circuits $C_0', C_1' \colon \mathbf{D}(\mathcal{O} \otimes \mathcal{G}) \to \mathbf{D}(\mathcal{A})$ given by

$$C_i'(\rho) = \operatorname{tr}_{\mathcal{I}} U_i^\dagger \rho U_i,$$

which is, the circuit C_i' simply runs the unitary U_i in reverse and traces out the space $\mathcal{I}$. To obtain the final circuits C_i we simply measure the output of C_i' in the computational basis and output 1 if the result is $|0\rangle$ and 0 otherwise. Informally, the circuit C_i simply runs Q_i backwards and accepts (outputs 1) if and only if the result is a valid initial configuration for the circuit Q_i, i.e. the space of the 'ancillary' qubits in $\mathcal{A}$ is $|0\rangle$. The pair (C_0, C_1) is the constructed instance of Π.

If (Q_0, Q_1) is a yes-instance of Close Images, then $(Q_0, Q_1) \in \Pi_Y$. To see this, take the states $\sigma_0, \sigma_1 \in \mathbf{D}(\mathcal{I})$ such that $Q_0(\sigma_0) = Q_1(\sigma_1)$. Let $\rho^i = U_i(\sigma_i \otimes |0\rangle\langle 0|)U_i^\dagger$ be the state obtained by running the circuit Q_i and not tracing out the space $\mathcal{G}$. This implies that the reduced states of ρ^0 and ρ^1 on the space $\mathcal{O}$ are equal. Furthermore, notice that

$$C_i'(\rho^i) = \operatorname{tr}_{\mathcal{I}} U_i^\dagger \rho^i U_i = \operatorname{tr}_{\mathcal{I}} U_i^\dagger (U_i(\sigma_i \otimes |0\rangle\langle 0|)U_i^\dagger)U_i = |0\rangle\langle 0|,$$

and so on these states the circuits C_0, C_1 output 1 with certainty, which implies that $(C_0, C_1) \in \Pi_Y$.

On the other hand, if (Q_0, Q_1) is a no-instance of Close Images, we show that the constructed instance belongs to Π_N. This argument is more technical. First we compute the acceptance probability of C_i on a state ρ, which is given by

$$\Pr[C_i(\rho) = 1] = \operatorname{tr}(|0\rangle\langle 0| \operatorname{tr}_{\mathcal{I}}(U_i^\dagger \rho U_i)) = \mathrm{F}(|0\rangle\langle 0|, \operatorname{tr}_{\mathcal{I}} U_i^\dagger \rho U_i)^2.$$

We then apply Uhlmann's theorem to conclude that, for some fixed purification $|\phi\rangle \in \mathcal{A} \otimes \mathcal{I} \otimes \mathcal{F}$ of $U_i^\dagger \rho U_i$, this quantity is equal to

$$\begin{aligned}
\max_{|\psi\rangle \in \mathcal{I} \otimes \mathcal{F}} \mathrm{F}(|0\rangle\langle 0| \otimes |\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|)^2 &\leq \max_{\sigma \in \mathbf{D}(\mathcal{I})} \mathrm{F}(|0\rangle\langle 0| \otimes \sigma, U_i^\dagger \rho U_i)^2 \\
&= \max_{\sigma \in \mathbf{D}(\mathcal{I})} \mathrm{F}(U_i|0\rangle\langle 0| \otimes \sigma U_i^\dagger, \rho)^2 \\
&\leq \max_{\sigma \in \mathbf{D}(\mathcal{I})} \mathrm{F}(C_i(\sigma), \operatorname{tr}_{\mathcal{G}} \rho)^2,
\end{aligned}$$

where we have made repeated use of the monotonicity of the fidelity with respect to the partial trace. Using this result, we have, for any two states ρ^0, ρ^1 such that $\operatorname{tr}_{\mathcal{G}} \rho^0 = \xi = \operatorname{tr}_{\mathcal{G}} \rho_1$

$$\begin{aligned}
\Pr[C_0(\rho^0) = 1] + \Pr[C_1(\rho^1) = 1] &\leq \max_{\sigma_0, \sigma_1} \mathrm{F}(C_0(\sigma_0), \xi)^2 + \mathrm{F}(C_1(\sigma_1), \xi)^2 \\
&\leq 1 + \max_{\sigma_0, \sigma_1} \mathrm{F}(C_0(\sigma_0), C_1(\sigma_1)) \\
&\leq 1 + 2^{-n},
\end{aligned}$$

where the penultimate inequality is by Lemma 8. This implies that $(Q_0, Q_1) \in \Pi_N$, and since this reduction is easily implemented in polynomial time, this implies that the problem Π is complete for QIP. ■

9.1.5 Quantum zero-knowledge proofs

The complexity class QSZK, introduced in [Wat02], is the class of all problems that can be interactively verified by a quantum verifier who learns nothing beyond the truth of the assertion being verified. In the case that the verifier is *honest*, i.e. does not deviate from the protocol in an attempt to gain information, this class can be defined in the following way.

Definition 20 *A language $L \in \mathsf{QSZK}_{\mathsf{HV}}$ if*

1. *There is a quantum interactive proof system for L.*
2. *The state of the verifier in this proof system after the sending of each message can be approximated, within negligible trace distance, by a polynomial-time preparable quantum state.*

If we insist that Item 2 holds even when the Verifier departs from the protocol, the result is the class QSZK. Watrous has shown that these two notions give the same complexity class, i.e. that $\mathsf{HVQSZK} = \mathsf{QSZK}$ [Wat09].

This definition of QSZK is somewhat informal. Fortunately this class has complete problems. This will allow us to work with this class without considering a completely formal definition.

Definition 21 (QSD Problem) *Let μ a negligible function. We define the promise problem $\mathrm{QSD} = \{\mathrm{QSD}_Y, \mathrm{QSD}_N\}$ as follows*

- *Input: two unitary quantum circuits C_0, C_1 of size n and m output qubits.*
- $(C_0, C_1) \in \mathrm{QSD}_Y \Leftrightarrow \| \rho^{C_0} - \rho^{C_1} \|_{\mathrm{tr}} \geq 2 - \mu(n)$
- $(C_0, C_1) \in \mathrm{QSD}_N \Leftrightarrow \| \rho^{C_0} - \rho^{C_1} \|_{\mathrm{tr}} \leq \mu(n)$

The promise problem QSD is QSZK-complete [Wat02].

9.1.6 Quantum computational distinguishability

The following definitions may be found in [Wat09].

Definition 22 *Two mixed states ρ^0 and ρ^1 on m qubits are (s, k, ε)-distinguishable if there exists a mixed state σ on k qubits and a quantum circuit D of size s that performs a binary outcome measurement on $(m + k)$ qubits, such that*

$$|\Pr[D(\rho^0 \otimes \sigma) = 1] - \Pr[D(\rho^1 \otimes \sigma) = 1]| \geq \varepsilon.$$

If ρ^0 and ρ^1 are not (s, k, ε)-distinguishable, then they are (s, k, ε)-indistinguishable.

Let $I \subseteq \{0,1\}^*$ and let an *auxiliary-input state ensemble* be a collection of mixed states $\{\rho_x\}_{x \in I}$ on $r(|x|)$ qubits for some polynomial r. These states have the further property that given x they can be generated in time $t(|x|)$, for some polynomial t.

Definition 23 *Two auxiliary-input state ensembles $\{\rho_x^0\}$ and $\{\rho_x^1\}$ on I are* quantum computationally indistinguishable *if for all polynomials p, s, k and for all but finitely many $x \in I$, the states ρ_x^0 and ρ_x^1 are $(s(|x|), k(|x|), 1/p(|x|))$-indistinguishable.*

The ensembles $\{\rho_x^0\}$ and $\{\rho_x^1\}$ on I are quantum computationally distinguishable *if there exist polynomials p, s, k such that for all $x \in I$, the states ρ_x^0 and ρ_x^1 are $(s(|x|), k(|x|), 1/p(|x|))$-distinguishable.*

If two ensembles are computationally distinguishable, then for all x there exists an efficient procedure in $|x|$ that distinguishes ρ_x^0 and ρ_x^1 with probability at least $1/2 + 1/p(|x|)$. Note that this is not a uniform procedure: the circuit that distinguishes the two states may depend on x.

We also define the statistical case

Definition 24 *Two auxiliary-input state ensembles $\{\rho_x^0\}$ and $\{\rho_x^1\}$ on I are* quantum statistically indistinguishable *if for any polynomial p and for all but finitely many $x \in I$,*

$$||\rho_x^0 - \rho_x^1||_{tr} \leq \frac{1}{p(|x|)}$$

Definition 25 *Two admissible superoperators Φ^0 and Φ^1 from t qubits to m qubits are (s, k, ε)-distinguishable if there exists a mixed state σ on $t + k$ qubits and a quantum circuit D of size s that performs a binary outcome measurement on $(m + k)$ qubits, such that*

$$|\Pr[D((\Phi^0 \otimes \mathbb{1}_k)(\sigma)) = 1] - \Pr[D((\Phi^1 \otimes \mathbb{1}_k)(\sigma)) = 1]| \geq \varepsilon,$$

where $\mathbb{1}_k$ denotes the identity superoperator on k qubits. If the superoperators Φ^0 and Φ^1 are not (s, k, ε)-distinguishable, then they are (s, k, ε)-indistinguishable.

Let $I \subseteq \{0,1\}^*$ and let an *auxiliary-input superoperator ensemble* be a collection of superoperators $\{\Phi_x\}_{x \in I}$ from $q(|x|)$ to $r(|x|)$ qubits for some polynomials q, r, where as in the case of state ensembles given x the superoperators can be performed efficiently in $|x|$.

Definition 26 *Two auxiliary-input superoperator ensembles $\{\Phi_x^0\}$ and $\{\Phi_x^1\}$ on I are* quantum computationally indistinguishable *if for all polynomials p, s, k and for all but finitely many $x \in I$, Φ_x^0 and Φ_x^1 are $(s(|x|), k(|x|), 1/p(|x|))$-indistinguishable.*

Two auxiliary-input state ensembles $\{\Phi_x^0\}$ and $\{\Phi_x^1\}$ on I are quantum computationally distinguishable *if there exist polynomials p, s, k such that for all $x \in I$ the superoperators Φ_x^0 and Φ_x^1 are $(s(|x|), k(|x|), 1/p(|x|))$-distinguishable.*

If two superoperator ensembles are computationally distinguishable then there exists an efficient procedure (in $|x|$) to distinguish them with probability at least $1/2 + 1/p(|x|)$ for some polynomial p. As in the case of state ensembles, this procedure is not necessarily uniform.

If the property of being (s, k, ε)-indistinguishable holds for all s, then we call an ensemble statistically-indistinguishable.

Let us note, that these definitions provide a strong quantum analogue of the classical non-uniform notion of computational indistinguishability, since the non-uniformity includes an arbitrary quantum state as advice to the quantum distinguisher.

We now define a new notion that we will use later on. Intuitively, we say that two circuits that take as input mixed states on the space $\mathcal{X} \otimes \mathcal{Y}$ and output a single bit are witnessable if there exist two input states that are equal on the space $\mathcal{Y}$ that are accepted respectively from the two circuits with high enough probability. More formally,

Definition 27 *Two superoperators Φ^0 and Φ^1 from $\mathbf{L}(\mathcal{X} \otimes \mathcal{Y})$ to a single bit are (s,k,p)-witnessable if there exist two input states $\rho^0, \rho^1 \in \mathbf{L}(\mathcal{X} \otimes \mathcal{Y})$ such that*

1. $$\frac{1}{2}\left(\Pr[\Phi^0(\rho^0) = 1] + \Pr[\Phi^1(\rho^1) = 1]\right) \geq 1/2 + \frac{1}{p(n)}$$

2. *there exists a state $\sigma \in \mathbf{L}(\mathcal{W})$ with $|\mathcal{W}| = k$ and an admissible superoperator $\Psi : \mathbf{L}(\mathcal{W} \otimes \mathcal{X}) \to \mathbf{L}(\mathcal{X})$ of size s, such that*

$$\rho^1 = (\Psi \otimes I_{\mathcal{Y}})(\sigma \otimes \rho^0)$$

where $I_{\mathcal{Y}}$ denotes the identity superoperator on $\mathbf{L}(\mathcal{Y})$.

If the superoperators Φ^0 and Φ^1 are not (s,k,p)-witnessable, then they are (s,k,p)-unwitnessable.

Let $I \subseteq \{0,1\}^*$ and let an *auxiliary-input superoperator ensemble* be a collection of superoperators $\{\Phi_x\}_{x \in I}$ from $q(|x|)$ to 1 bit for some polynomial q, where given x the superoperators can be performed efficiently in $|x|$.

Definition 28 *Two auxiliary-input superoperator ensembles $\{\Phi_x^0\}$ and $\{\Phi_x^1\}$ on I are quantum computationally witnessable if there exist polynomials s, k, p such that for all $x \in I$ the superoperators Φ_x^0 and Φ_x^1 are $(s(|x|), k(|x|), p(|x|))$-witnessable.*

Two auxiliary-input superoperator ensembles $\{\Phi_x^0\}$ and $\{\Phi_x^1\}$ on I are quantum computationally unwitnessable if for all polynomials s, k, p and for all but finitely many $x \in I$ the superoperators Φ_x^0 and Φ_x^1 are $(s(|x|), k(|x|), p(|x|))$-unwitnessable.

9.1.7 Quantum commitments

Definition 29 *A quantum commitment scheme (resp. with quantum advice) is an interactive protocol $Com = (S, R)$ with the following properties*

- *The sender S and the receiver R have common input a security parameter 1^n (resp. both S and R have a copy of a quantum state $|\phi\rangle$ of $\mathrm{poly}(n)$ qubits). The receiver has private input the bit $b \in \{0,1\}$ to be committed. Both S and R are quantum algorithms that run in time $\mathrm{poly}(n)$.*

- *In the* commit *phase, the sender S interacts with the receiver R in order to commit to b.*

- *In the* reveal *phase, the sender S interacts with the receiver R in order to reveal b. The receiver R decides to accept or reject depending on the revealed value of b and his final state. We say that S reveals b, if R accepts the revealed value. In the honest case, R always accepts.*

A commitment scheme is non-interactive *if both the commit and the reveal phase consist of a single message from the sender to the receiver.*

When the commit phase is non-interactive, we call ρ_S^b the state sent by the honest sender during the commit phase if his input bit is b.

Since we will only consider non-interactive commitments, we define auxiliary-input quantum commitment schemes only for the non-interactive case.

Definition 30 *A* non-interactive auxiliary-input quantum commitment scheme (resp. with quantum advice) on I *which is statistically/computationally hiding and statistically/computationally binding is a collection of non-interactive quantum commitment schemes (resp. with quantum advice)* $\mathcal{C} = \{Com_x = (S_x, R_x)\}_{x \in I}$ *with the following properties*

- *there exists a quantum circuit* Q *of size polynomial in* $|x|$*, that given as input* x *for any* $x \in I$*, can apply the same maps that* S_x *and* R_x *apply during the commitment scheme in time polynomial in* $|x|$*.*
- *(statistically/computationally hiding) the two auxiliary-input state ensembles* $\{\rho^0_{S_x}\}_{x \in I}$ *and* $\{\rho^1_{S_x}\}_{x \in I}$ *are quantum statistically/computationally indistinguishable.*
- *(statistically/computationally binding) for all but finitely many* $x \in I$*, for all polynomial* p *and for any unbounded/polynomial dishonest sender* S^*_x*, we have*

$$P_{S^*_x} = \frac{1}{2}\left(\Pr[S^*_x \text{ reveals } b = 0] + \Pr[S^*_x \text{ reveals } b = 1]\right) \leq \frac{1}{2} + \frac{1}{p(|x|)}$$

When referring to a commitment scheme, we will use the (b_s, h_c) and (b_c, h_s) to denote schemes that are statistically binding-computationally hiding and computationally binding-statistically hiding, respectively.

In high level, the distinction between the two notions, with or without advice, is the following. We can assume that the two players decide to perform a commitment scheme and agree on a security parameter n. Then, in the first case, a trusted party can give them the description of the circuits (C_0, C_1) so that the players can perform the commitment scheme themselves. One can think of the string (C_0, C_1) as a classical advice to the players. In the second case, the trusted party gives them the description of the circuits, as well as one copy of a quantum state each. This quantum state is of polynomial size, however it is not efficiently constructable, otherwise the trusted party could have given the players the classical description of the circuit that constructs it. Hence, in the second notion the players receive both classical and quantum advice.

9.2 Quantum commitments unless QSZK $\subseteq$ QMA

Theorem 15 *If* QSZK $\not\subseteq$ QMA*, then there exists a non-interactive auxiliary-input quantum* (b_s, h_c)*-commitment scheme on an infinite set* I*.*

Proof: First, we show the following

Lemma 7 *If* QSZK $\not\subseteq$ QMA *then there exist two auxiliary-input state ensembles that are quantum computationally indistinguishable on an infinite set* I*.*

Proof: Let us consider the complete problem $\text{QSD} = \{\text{QSD}_Y, \text{QSD}_N\}$ for QSZK_{HV}. We may restrict attention to the honest verifier case, since it is known that QSZK $=$ QSZK_{HV} [Wat09]. Let $n = |(C_0, C_1)|$ and define $|\phi_{C_b}\rangle = C_b(|0\rangle)$

in the space $\mathcal{O} \otimes \mathcal{G}$ to be the entire output state of the circuit on input $|0\rangle$ and $\rho^{C_b}_{(C_0,C_1)} = \mathrm{Tr}_{\mathcal{G}}(|\phi_{C_b}\rangle\langle\phi_{C_b}|)$ be the output of circuit C_b on $m(n)$ qubits for a polynomial m.

Recall that the set QSD_Y consists of pairs of circuits (C_0, C_1), such that the trace norm satisfies $\| \rho^{C_0}_{(C_0,C_1)} - \rho^{C_1}_{(C_0,C_1)} \|_{\mathrm{tr}} \geq 2-\mu(n)$. We now consider the two auxiliary-input state ensembles $\{\rho^{C_0}_{(C_0,C_1)}\}$ and $\{\rho^{C_1}_{(C_0,C_1)}\}$ for $(C_0, C_1) \in \mathrm{QSD}_Y$. Assume for contradiction that they are quantum computationally distinguishable on QSD_Y, i.e. for some polynomials p, s, k and for all $(C_0, C_1) \in \mathrm{QSD}_Y$, the states $\rho^{C_0}_{(C_0,C_1)}$ and $\rho^{C_1}_{(C_0,C_1)}$ are $(s(n), k(n), 1/p(n))$-distinguishable. In other words, for polynomials p, s, k and for all $(C_0, C_1) \in \mathrm{QSD}_Y$ there exists a mixed state σ on $k(n)$ qubits and a quantum circuit Q of size $s(n)$ that performs a binary outcome measurement on $m(n) + k(n)$ qubits, such that

$$|\Pr[Q(\rho^{C_0}_{(C_0,C_1)} \otimes \sigma) = 1] - \Pr[Q(\rho^{C_1}_{(C_0,C_1)} \otimes \sigma) = 1]| \geq \frac{1}{p(n)}.$$

We now claim that this implies that $\mathsf{QSZK} \subseteq \mathsf{QMA}$, which is a contradiction. For any input (C_0, C_1) the prover can send the classical polynomial size description of Q to the verifier as well as the mixed state σ with polynomial number of qubits. Then, for all $(C_0, C_1) \in \mathrm{QSD}_Y$, the verifier with the help of Q and σ can distinguish between the two circuits with probability higher than $\frac{1}{2} + \frac{1}{2p(n)}$. On the other hand, for all $(C_0, C_1) \in \mathrm{QSD}_N$, no matter what Q and σ the prover sends, since $\| \rho^{C_0}_{(C_0,C_1)} - \rho^{C_1}_{(C_0,C_1)} \|_{\mathrm{tr}} \leq \mu(n)$ the verifier can only distinguish the two circuits with probability at most $\frac{1}{2} + \frac{\mu(n)}{2}$. This implies that there is an inverse polynomial gap between the acceptance probabilities in the two cases. By applying standard error reduction tools for QMA [KSV02, MW05], we obtain a QMA protocol to solve QSD.

This implies that if $\mathsf{QSZK} \not\subseteq \mathsf{QCMA}$ then there exists a non empty set $I \subseteq \mathrm{QSD}_Y$ such that the two auxiliary-input state ensembles $\{\rho^{C_0}_{(C_0,C_1)}\}$ and $\{\rho^{C_1}_{(C_0,C_1)}\}$ are quantum computationally indistinguishable on I. Notice that the set I is infinite. Indeed, if I is finite, then by hard-wiring this finite number of instances into the QMA verifier (who always accepts these instances), we have again that $\mathsf{QSZK} \subseteq \mathsf{QMA}$. ■

We now show how to construct a commitment scheme from these ensembles

Lemma 8 *The two auxiliary-input state ensembles $\{\rho^{C_0}_{(C_0,C_1)}\}_{(C_0,C_1)\in I}$ and $\{\rho^{C_1}_{(C_0,C_1)}\}_{(C_0,C_1)\in I}$ that are quantum computationally indistinguishable on the infinite set I imply a non-interactive auxiliary-input quantum (b_s, h_c)-commitment scheme on I.*

Proof:

For every $(C_0, C_1) \in I$ we define the following commitment scheme

- Define $n = |(C_0, C_1)|$ to be the security parameter.
- Commit phase: To commit to bit b, the sender S runs the quantum circuit C_b with input $|0\rangle$ to create $|\phi_{C_b}\rangle = C_b(|0\rangle)$ and sends $\rho^{C_b}_{(C_0,C_1)}$ to the receiver R, which is the portion of $|\phi_{C_b}\rangle$ in the space $\mathcal{O}$.
- Reveal phase: To reveal bit b, the sender S sends the remaining qubits of the state $|\phi_{C_b}\rangle$ to the receiver R, which lie in the space $\mathcal{G}$ (the honest

sender sends $|\phi'\rangle = C_b|0\rangle$). The receiver applies the circuit $C_b^\dagger$ on his entire state and then measures all his qubits in the computational basis. He accepts if and only if the outcome is $|0\rangle$.

Let us analyze the above scheme. First, note that all operations of the sender and the receiver in the above protocol can be computed in time polynomial in n given the input (C_0, C_1). This includes the receiver's test during the reveal phase.

Moreover, it is computationally hiding since the states $\{\rho^{C_0}_{(C_0,C_1)}\}$ and $\{\rho^{C_1}_{(C_0,C_1)}\}$ are quantum computationally indistinguishable.

The fact that the protocol is statistically binding follows from the fact that for the states $\{\rho^{C_0}_{(C_0,C_1)}\}$ and $\{\rho^{C_1}_{(C_0,C_1)}\}$ (for $(C_0, C_1) \in I \subseteq \mathrm{QSD}_Y$) we have $\| \rho^{C_0}_{(C_0,C_1)} - \rho^{C_1}_{(C_0,C_1)} \|_{\mathrm{tr}} \geq 2 - \mu(n)$, for a negligible function μ. More precisely, if ξ is the total quantum state sent by a dishonest sender S^* in the commit and reveal phase of the protocol, then the probability that ξ can be revealed as the bit b is bounded by

$$\Pr[S^* \text{ reveals } b \text{ from } \xi] = \mathrm{tr}(|0\rangle\langle 0| C_b^\dagger \xi C_b) = \mathrm{F}(C_b(|0\rangle), \xi)^2 \leq \mathrm{F}(\rho^{C_b}_{(C_0,C_1)}, \mathrm{tr}_{\mathcal{G}}\, \xi)^2$$

using the monotonicity of the fidelity with respect to the partial trace. This calculation follows the proof of Watrous that QSZK is closed under complementation [Wat02]. Using this fact, as well as the property of the fidelity given in Lemma 8, we have

$$\begin{aligned} P_{S^*} &= \frac{1}{2}\left(\Pr[S^* \text{ reveals } b = 0] + \Pr[S^* \text{ reveals } b = 1]\right) \\ &\leq \max_{\xi} \frac{1}{2}\left(\mathrm{F}(\rho^{C_0}_{(C_0,C_1)}, \mathrm{tr}_{\mathcal{G}}\, \xi)^2 + \mathrm{F}(\rho^{C_1}_{(C_0,C_1)}, \mathrm{tr}_{\mathcal{G}}\, \xi)^2\right) \\ &= \frac{1}{2}\left(1 + \mathrm{F}(\rho^{C_0}_{(C_0,C_1)}, \rho^{C_1}_{(C_0,C_1)})\right) \\ &\leq \frac{1}{2} + \frac{\sqrt{\mu(n)}}{2}, \end{aligned}$$

where the final inequality follows from Lemma 9 and the fact that the trace distance of the two states satisfies $\| \rho^{C_0}_{(C_0,C_1)} - \rho^{C_1}_{(C_0,C_1)} \|_{\mathrm{tr}} \geq 2 - \mu(n)$. This implies that the protocol is statistically binding. ■

By combining the above two Lemmata, we conclude that if QSZK $\not\subseteq$ QMA, then there exists a non-interactive auxiliary-input quantum (b_s, h_c)-commitment scheme on an infinite set I. ■

Note, that if we are willing to relax the indistinguishability condition, i.e. enforce the indistinguishability of the states against a quantum algorithm that has only classical auxiliary input (i.e. get rid of the state ξ), then the condition becomes QSZK $\not\subseteq$ QCMA. Notice also that by using a result of Crépeau, Légaré, and Salvail [CLS01] we can convert this commitment scheme into one that is statistically hiding and computationally binding.

9.3 Quantum (b_s, h_c)-commitments unless QIP $\subseteq$ QMA

First, let us note that the condition QIP $\subseteq$ QMA implies that PSPACE $\subseteq$ PP which is widely believed not to be true. Hence, the commitment we exhibit are based on a very weak classical computational assumption. Of course, since the result is so strong, the commitments themselves are weaker, in the sense that apart from a classical advice, one needs a quantum advice as well in order to construct them. Note of course, that our definitions of security are against quantum adversaries that also receive an arbitrary quantum advice, hence our honest players are not more powerful than the dishonest ones. Moreover, the quantum advice does not create entanglement between the two players.

The proof is very similar to the previous one. The first protocol that we obtain is based on the swap test on two nearly orthogonal states. For this reason a cheating Sender can open either zero or one with probability $3/4 + \mathrm{neg}(n)$. Following the proof of this Theorem (in Proposition 25 we show how to repeat the protocol in parallel to obtain negligible binding error.

Theorem 16 *If* QIP $\not\subseteq$ QMA*, then there exists a non-interactive auxiliary-input quantum (b_s, h_c)-commitment scheme with quantum advice on an infinite set I. This scheme has constant binding error.*

Proof: We first show the following

Lemma 9 *If* QIP $\not\subseteq$ QMA*, there exist two auxiliary-input superoperator ensembles $\{Q^0\}_{(Q^0,Q^1)\in I}$ and $\{Q^1\}_{(Q^0,Q^1)\in I}$ that are quantum computationally indistinguishable on an infinite set I.*

Proof: Suppose QIP $\not\subseteq$ QMA. Let us consider the complete problem QCD for QIP with input the mixed-state circuits (Q^0, Q^1). Let $n = |(Q^0, Q^1)|$. Let $\mathcal{I}$ denote the input space, $\mathcal{O}$ the output space and $\mathcal{G}$ the output garbage space of the circuits Q^0, Q^1.

Consider the set QCD_Y, whose elements are pairs of circuits (Q^0, Q^1), such that the diamond norm satisfies $\| Q^0 - Q^1 \|_\diamond \geq 2 - \mu(n)$, and the two auxiliary-input superoperator ensembles $\{Q^0\}_{(Q^0,Q^1)\in \mathrm{QCD}_Y}$ and $\{Q^1\}_{(Q^0,Q^1)\in \mathrm{QCD}_Y}$. Assume for contradiction that they are quantum computationally distinguishable on QCD_Y, i.e. for some polynomials p, s, k and all $(Q^0, Q^1) \in \mathrm{QSD}_Y$, the superoperators Q^0 and Q^1 are $(s(n), k(n), 1/p(n))$-distinguishable. In other words, for polynomials p, s, k and for all $(Q^0, Q^1) \in \mathrm{QSD}_Y$ there exists a mixed state σ on $t(n) + k(n)$ qubits and a quantum circuit D of size $s(n)$ that performs a binary outcome measurement on $(m(n) + k(n))$ qubits, such that

$$|\Pr[D((Q^0 \otimes \mathbb{1}_k)(\sigma)) = 1] - \Pr[D((Q^1 \otimes \mathbb{1}_k)(\sigma)) = 1]| \geq \frac{1}{p(n)}$$

We now claim that this implies that QIP $\subseteq$ QMA, which is a contradiction. For any input (Q^0, Q^1) the QMA-prover can send to the verifier the classical polynomial size description of D as well as the mixed state σ with $\mathrm{poly}(n)$ qubits. Then, for all $(Q^0, Q^1) \in \mathrm{QCD}_Y$, the verifier with the help of D and σ can distinguish between the two circuits with probability higher than $\frac{1}{2} + \frac{1}{2p(n)}$. On the other hand, for all $(Q^0, Q^1) \in \mathrm{QCD}_N$, no matter what D and

σ the prover sends, since $\| Q^0 - Q^1 \|_\diamond \leq \mu(n)$ the verifier can only distinguish the two circuits with probability at most $\frac{1}{2} + \frac{\mu(n)}{2}$. Hence, there is at least an inverse polynomial gap between the two probabilities, so we can use error reduction [KSV02, MW05] to obtain a QMA protocol that solves QCD with high probability.

We just showed that QIP $\not\subseteq$ QMA implies that there exists a non-empty set $I \subseteq \mathrm{QCD}_Y$ and two auxiliary-input superoperator ensembles $\{Q^0\}_{(Q^0,Q^1)\in \mathrm{QCD}_Y}$ and $\{Q^1\}_{(Q^0,Q^1)\in \mathrm{QCD}_Y}$ which are quantum computationally indistinguishable on I. Once again, the set I must be infinite, as if I is finite then by hard-wiring this finite number of instances into the QMA verifier (who always accepts these instances), we have again that QIP $\subseteq$ QMA. ■

We now need to show how to construct a commitment scheme on I based on these indistinguishable superoperator ensembles. The protocol we obtain has only constant binding error: the average of the probability of successfully revealing 0 and the probability of successfully revealing 1 is negligibly larger than 3/4. Following this Lemma we prove a parallel repetition result for this protocol that reduces this error to a negligible function.

Lemma 10 *The two auxiliary-input superoperator ensembles $\{Q^0\}_{(Q^0,Q^1)\in I}$ and $\{Q^1\}_{(Q^0,Q^1)\in I}$, which are quantum computationally indistinguishable on the infinite set $I \subseteq \mathrm{QCD}_Y$, imply a non-interactive auxiliary-input quantum (b_s, h_c)-commitment scheme with quantum advice on I. This protocol has constant binding error.*

Proof: For every $(Q^0, Q^1) \in I$ we define a quantum commitment scheme with quantum advice. For convenience we let U^b be the unitary operation that simulates the admissible map Q^b, in other words we have that $Q^b(\rho) = \mathrm{tr}_G\, U^b(\rho \otimes |0\rangle\langle 0|)(U^b)^\dagger$. Note that any Q^b can be efficiently converted to a unitary circuit U^b. Let also $|\phi^*\rangle$ be the pure state from Lemma 1, such that

$$\| Q^0 - Q^1 \|_\diamond = \| (I_\mathcal{F} \otimes (Q^0 - Q^1))(|\phi^*\rangle\langle\phi^*|) \|_{\mathrm{tr}}.$$

- Define $n = |(Q^0, Q^1)|$ to be the security parameter. S and R also receive as advice a copy of the state $|\phi^*\rangle$ on poly(n) qubits.

- Commit phase: To commit to bit b, the sender S runs the quantum circuit $\mathbb{1}_\mathcal{F} \otimes U^b$ with input $|\phi^*\rangle|0\rangle$. The entire output of the circuit is a state in the space $\mathcal{F}\otimes\mathcal{O}\otimes\mathcal{G}$. The sender then sends the qubits in the space $\mathcal{O}\otimes\mathcal{F}$ to the receiver R.

- Reveal phase: To reveal bit b, the sender S sends the remaining qubits of the state $(\mathbb{1}_\mathcal{F}\otimes U^b)(|\phi^*\rangle|0\rangle)$ in the space $\mathcal{G}$ to the receiver R. The receiver first applies the operation $\mathbb{1}_\mathcal{F} \otimes (U^b)^\dagger$ to the entire state he received from the sender and then performs a swap test between this state and his copy of $|\phi^*\rangle|0\rangle$.

Let us analyze the above scheme. First, note that all operations of the sender and the receiver in the above protocol can be computed in time polynomial in n given the input (Q^0, Q^1). This includes the receiver's test during the reveal phase, since given a description of a unitary circuit it can be inverted by simply

taking the inverse of each gate and running the circuit in reverse and the swap test which is also efficient.

The protocol is computationally hiding since the superoperators Q^0 and Q^1 are quantum computationally indistinguishable.

The fact that the protocol is statistically binding (with constant error) follows from the fact that we have $\| Q^0 - Q^1 \|_\diamond \geq 2 - \mu(n)$ for a negligible function μ. More precisely, let σ^b be the state sent by the sender with $\mathrm{tr}_{\mathcal{G}}\, \sigma^0 = \mathrm{tr}_{\mathcal{G}}\, \sigma^1 = \sigma_{\mathcal{OF}}$ (the honest sender sends the pure state $(\mathbb{1}_{\mathcal{F}} \otimes U^b)(|\phi^*\rangle|0\rangle)$). Then the receiver accepts if and only if the output of $(\mathbb{1}_{\mathcal{F}} \otimes (U^b)^\dagger)\sigma^b(\mathbb{1}_{\mathcal{F}} \otimes U_b)$ and his copy of $|\phi^*\rangle|0\rangle$ pass the swap test. This probability is equal to

$$\begin{aligned}
\Pr[S^* \text{ reveals } b \text{ from } \sigma^b] &= \frac{1}{2} + \frac{1}{2}\,\mathrm{tr}\left[(|\phi^*\rangle\langle\phi^*| \otimes |0\rangle\langle 0|)(\mathbb{1}_{\mathcal{F}} \otimes (U^b)^\dagger)\sigma^b(\mathbb{1}_{\mathcal{F}} \otimes U_b)\right] \\
&= \frac{1}{2} + \frac{1}{2}\,\mathrm{F}((\mathbb{1}_{\mathcal{F}} \otimes U_b)(|\phi^*\rangle\langle\phi^*| \otimes |0\rangle\langle 0|)(\mathbb{1}_{\mathcal{F}} \otimes (U^b)^\dagger), \sigma^b)^2 \\
&\leq \frac{1}{2} + \frac{1}{2}\,\mathrm{F}(\mathbb{1}_{\mathcal{F}} \otimes Q^b(|\phi^*\rangle\langle\phi^*|), \mathrm{tr}_{\mathcal{G}}\, \sigma^b)^2 \\
&\leq \frac{1}{2} + \frac{1}{2}\,\mathrm{F}(\mathbb{1}_{\mathcal{F}} \otimes Q^b(|\phi^*\rangle\langle\phi^*|), \sigma_{\mathcal{OF}})^2
\end{aligned}$$

where we have used the fact that the swap test on a state $\rho \otimes \sigma$ returns the symmetric outcome with probability $\frac{1}{2} + \frac{1}{2}\,\mathrm{tr}\,\rho\sigma$, as well as the monotonicity of the fidelity with respect to the partial trace.

Using this calculation, the binding property of the protocol is given by

$$\begin{aligned}
P_{S^*} &= \frac{1}{2}\left(\Pr[S^* \text{ reveals } b = 0] + \Pr[S^* \text{ reveals } b = 1]\right) \\
&\leq \frac{1}{2} + \frac{1}{4}\left(\mathrm{F}(\mathbb{1}_{\mathcal{F}} \otimes Q^0(|\phi^*\rangle\langle\phi^*|), \mathrm{tr}_{\mathcal{G}}\, \sigma)^2 + \mathrm{F}(\mathbb{1}_{\mathcal{F}} \otimes Q^1(|\phi^*\rangle\langle\phi^*|), \mathrm{tr}_{\mathcal{G}}\, \sigma)^2\right) \\
&\leq \frac{1}{2} + \frac{1}{4}\left(1 + \mathrm{F}(\mathbb{1}_{\mathcal{F}} \otimes Q^0(|\phi^*\rangle\langle\phi^*|), \mathbb{1}_{\mathcal{F}} \otimes Q^1(|\phi^*\rangle\langle\phi^*|))\right) \\
&\leq \frac{3}{4} + \frac{\sqrt{\mu(n)}}{4},
\end{aligned}$$

where we have used Lemma 1 and Lemma 8. ■

From the above two Lemmata, we almost have that if $\mathsf{QIP} \not\subseteq \mathsf{QMA}$, then there exists a non-interactive auxiliary-input quantum (b_s, h_c)-commitment scheme with quantum advice on an infinite set I, with constant binding error. The only thing to do is to reduce the cheating probability of the sender to $1/2 + \mathrm{neg}(n)$. To do this, we will use parallel repetition of the above protocol.

Proposition 25 *Consider a k-fold repetition of the above bit commitment protocol. This protocol is a non-interactive auxiliary-input quantum (b_s, h_c)-commitment scheme with quantum advice on I.*

Proof: The two things we have to make sure of is that the computationally hiding property remains under parallel repetition and that the cheating probability of the sender decreases as a negligible function in k. To show that the protocol is computationally hiding, we use the following Lemma.

Lemma 11 ([Wat09]) *Suppose that $\rho_1, \ldots \rho_n$ and $\xi_1, \ldots, \xi_n$ are m-qubit states such that $\rho_1 \otimes \cdots \otimes \rho_n$ and $\xi_1 \otimes \cdots \otimes \xi_n$ are (s, k, ε)-distinguishable. Then there*

exists at least one choice of $j \in \{1, \ldots, n\}$ *for which* ρ_j *and* ξ_j *are* $(s, (n-1)m + k, \varepsilon/n)$*-distinguishable.*

From this Lemma, we easily have that if the superoperators Q_0 and Q_1 are quantum computationally indistinguishable then the output states of the superoperators $Q_0^{\otimes k}$ and $Q_1^{\otimes k}$ applied to any product state are quantum computationally indistinguishable for any k of polynomial size. This proves that the repeated protocol remains computationally hiding, since the honest Sender prepares a product state.

We now need to prove that the statistical hiding property decreases to $1/2 + \mathrm{neg}(n)$. We first prove the following Lemma that applies to the ideal case, i.e. the Receiver applies the swap test to one of two states with orthogonal reduced states. The calculation that this strategy (approximately) generalizes to the case of states that are *almost* orthogonal states follows the proof of the Lemma.

Lemma 12 *Let* $|\phi_0\rangle, |\phi_1\rangle \in \mathcal{A} \otimes \mathcal{B}$ *be states such that* $\mathrm{tr}_{\mathcal{B}} |\phi_0\rangle\langle\phi_0|$ *and* $\mathrm{tr}_{\mathcal{B}} |\phi_1\rangle\langle\phi_1|$ *are orthogonal, and let* ρ_0, ρ_1 *be two states on* $(\mathcal{A} \otimes \mathcal{B})^{\otimes k} = \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \cdots \otimes \mathcal{A}_k \otimes \mathcal{B}_k$ *such that*

$$\mathrm{tr}_{\mathcal{B}_1 \otimes \cdots \otimes \mathcal{B}_k} \rho_0 = \mathrm{tr}_{\mathcal{B}_1 \otimes \cdots \otimes \mathcal{B}_k} \rho_1.$$

Consider the following test:

> *Test b: Take k copies of* $|\phi_b\rangle$ *and apply for each* $i \in \{1, \ldots, k\}$ *the swap test between each copy and the state in* $\mathcal{A}_i \otimes \mathcal{B}_i$*. Accept if all the swap tests accept.*

For any ρ_0 *and* ρ_1 *with equal reduced states on* $\mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_k$*, we have*

$$\frac{1}{2}\left(\Pr[\rho_0 \textit{ passes Test } 0] + \Pr[\rho_1 \textit{ passes Test } 1]\right) \leq \frac{1}{2} + \frac{1}{2^{k+1}}$$

Proof: [Proof of Lemma 12] We prove the result by induction on k. For $k = 1$. We have

$$\begin{aligned}
\Pr[\rho_b \text{ passes Test } b] &= 1/2 + \langle\phi_b|\rho_b|\phi_b\rangle/2 \\
&= 1/2 + \mathrm{F}(|\phi_b\rangle\langle\phi_b|, \rho_b)^2/2 \\
&\leq 1/2 + \mathrm{F}(\mathrm{tr}_{\mathcal{B}} |\phi_b\rangle\langle\phi_b|, \mathrm{tr}_{\mathcal{B}} \rho_b)^2/2.
\end{aligned}$$

Since $\mathrm{tr}_{\mathcal{B}} \rho_0 = \mathrm{tr}_{\mathcal{B}} \rho_1$, this implies that

$$\begin{aligned}
&\frac{1}{2}\left(\Pr[\rho_0 \text{ passes Test } 0] + \Pr[\rho_1 \text{ passes Test } 1]\right) \\
&\quad \leq \frac{1}{2} + \frac{1}{4}(\mathrm{F}(\mathrm{tr}_{\mathcal{B}} |\phi_0\rangle\langle\phi_0|, \mathrm{tr}_{\mathcal{B}} \rho_0)^2 + \mathrm{F}(\mathrm{tr}_{\mathcal{B}} |\phi_1\rangle\langle\phi_1|, \mathrm{tr}_{\mathcal{B}} \rho_1)^2) \\
&\quad \leq \frac{1}{2} + \frac{1}{4}(1 + \mathrm{F}(\mathrm{tr}_{\mathcal{B}} |\phi_0\rangle\langle\phi_0|, \mathrm{tr}_{\mathcal{B}} |\phi_1\rangle\langle\phi_1|)) = \frac{3}{4}
\end{aligned}$$

since the reduced states of $|\phi_0\rangle, |\phi_1\rangle$ are orthogonal.

Now we suppose the Lemma is true for k and show it for $k + 1$. For convenience we set $\mathcal{S}_i = \mathcal{A}_i \otimes \mathcal{B}_i$. We take a reference space $\mathcal{R}$ of sufficient size to consider purifications of ρ_0 and ρ_1. Let $\rho_b = \mathrm{tr}_{\mathcal{R}} |\psi_b\rangle\langle\psi_b|$ be these (arbitrary) purifications. Using this notation, we write

$$|\psi_0\rangle = \alpha_0 |\phi_0\rangle_{\mathcal{S}_1} |\Omega_0\rangle_{\mathcal{S}_2 \otimes \cdots \otimes \mathcal{S}_{k+1} \otimes \mathcal{R}} + \alpha_1 |\phi_1\rangle_{\mathcal{S}_1} |\Omega_1\rangle_{\mathcal{S}_2 \otimes \cdots \otimes \mathcal{S}_{k+1} \otimes \mathcal{R}} + \alpha_2 \sum_{i=2}^{n} |\phi_i\rangle |\Omega_i\rangle \tag{9.1}$$

and

$$|\psi_1\rangle = \beta_0|\phi_0\rangle_{\mathcal{S}_1}|\Gamma_0\rangle_{\mathcal{S}_2\otimes\cdots\otimes\mathcal{S}_{k+1}\otimes\mathcal{R}} + \beta_1|\phi_1\rangle_{\mathcal{S}_1}|\Gamma_1\rangle_{\mathcal{S}_2\otimes\cdots\otimes\mathcal{S}_{k+1}\otimes\mathcal{R}} + \beta_2\sum_{i=2}^{n}|\phi_i\rangle|\Gamma_i\rangle \tag{9.2}$$

where each $|\phi_i\rangle, |\phi_j\rangle$ are orthogonal for $i \neq j$ (for $|\phi_0\rangle$ and $|\phi_1\rangle$ this follows from the fact that the reduced states on $\mathcal{A}_1$ are orthogonal). Since the goal is to pass swap tests with $|\phi_0\rangle$ and $|\phi_1\rangle$, we can easily see that we can take $\alpha_2 = \beta_2 = 0$ without loss of generality, since this state will only have larger probability of passing the tests. As one final notational convenience, let $p_i = |\alpha_i|^2$ and $q_i = |\beta_i|^2$.

Before we analyze the probability that the swap tests pass, we show that the probabilities p_0 and q_1 satisfy $p_0 + q_1 \leq 1$. By Equation (9.1) we have

$$\begin{aligned} p_0 = |\alpha_0|^2 &= \operatorname{tr}((|\phi_0\rangle\langle\phi_0| \otimes \mathbb{1})|\psi_0\rangle\langle\psi_0|) \\ &\leq \mathrm{F}(|\phi_0\rangle\langle\phi_0|, \operatorname{tr}_{\mathcal{S}_2\ldots\mathcal{S}_{k+1}\mathcal{R}}|\psi_0\rangle\langle\psi_0|)^2 \\ &\leq \mathrm{F}(\operatorname{tr}_{\mathcal{B}_1}|\phi_0\rangle\langle\phi_0|, \operatorname{tr}_{\mathcal{B}_1\mathcal{S}_2\ldots\mathcal{S}_{k+1}\mathcal{R}}|\psi_0\rangle\langle\psi_0|)^2. \end{aligned}$$

By a similar calculation, we have

$$q_1 = |\beta_1|^2 \leq \mathrm{F}(\operatorname{tr}_{\mathcal{B}_1}|\phi_1\rangle\langle\phi_1|, \operatorname{tr}_{\mathcal{B}_1\mathcal{S}_2\ldots\mathcal{S}_{k+1}\mathcal{R}}|\psi_1\rangle\langle\psi_1|)^2.$$

Then, using the fact that $\operatorname{tr}_{\mathcal{B}_1\mathcal{S}_2\ldots\mathcal{S}_{k+1}\mathcal{R}}|\psi_0\rangle\langle\psi_0| = \operatorname{tr}_{\mathcal{B}_1\mathcal{S}_2\ldots\mathcal{S}_{k+1}\mathcal{R}}|\psi_1\rangle\langle\psi_1|$, as well as the fact that $\operatorname{tr}_{\mathcal{B}_1}|\phi_0\rangle\langle\phi_0|$ and $\operatorname{tr}_{\mathcal{B}_1}|\phi_1\rangle\langle\phi_1|$ are orthogonal, we have

$$\begin{aligned} p_0 + q_1 &\leq \mathrm{F}(\operatorname{tr}_{\mathcal{B}_1}|\phi_0\rangle\langle\phi_0|, \operatorname{tr}_{\mathcal{B}_1\mathcal{S}_2\ldots\mathcal{S}_{k+1}\mathcal{R}}|\psi_0\rangle\langle\psi_0|)^2 + \mathrm{F}(\operatorname{tr}_{\mathcal{B}_1}|\phi_1\rangle\langle\phi_1|, \operatorname{tr}_{\mathcal{B}_1\mathcal{S}_2\ldots\mathcal{S}_{k+1}\mathcal{R}}|\psi_1\rangle\langle\psi_1|)^2 \\ &\leq 1 + \mathrm{F}(\operatorname{tr}_{\mathcal{B}_1}|\phi_0\rangle\langle\phi_0|, \operatorname{tr}_{\mathcal{B}_1}|\phi_1\rangle\langle\phi_1|) \\ &= 1. \end{aligned} \tag{9.3}$$

We now analyze the probability that the swap tests pass. Consider applying test 0 on $|\psi_0\rangle$. When applying the swap test between $|\phi_0\rangle$ and $|\phi_0\rangle$, the result is the state $|0\rangle|\phi_0\rangle|\phi_0\rangle$ where the first register corresponds to the acceptance of the swap test (0 corresponds to accept). When applying the swap test between the two states $|\phi_0\rangle$ and $|\phi_1\rangle$, the result before measuring the first qubit is $\frac{1}{\sqrt{2}}(|0\rangle(|\phi_0\rangle|\phi_1\rangle + |\phi_1\rangle|\phi_0\rangle) + |1\rangle(|\phi_0\rangle|\phi_1\rangle - |\phi_1\rangle|\phi_0\rangle))$. So the swap test on the space $\mathcal{S}_1$ accepts with probability $p_0 + p_1/2$. Conditioned on this test passing, we have the state:

$$\frac{1}{\sqrt{p_0 + p_1/2}}\left[\alpha_0|\phi_0\rangle|\phi_0\rangle|\Omega_0\rangle_{\mathcal{S}_2\otimes\cdots\otimes\mathcal{S}_{k+1}\mathcal{R}} + \frac{\alpha_1}{\sqrt{2}}(|\phi_0\rangle|\phi_1\rangle + |\phi_1\rangle|\phi_0\rangle)|\Omega_1\rangle_{\mathcal{S}_2\otimes\cdots\otimes\mathcal{S}_{k+1}\mathcal{R}}\right]$$

Discarding the first system results in the state in $\mathcal{S}_2 \otimes \cdots \otimes \mathcal{S}_{k+1} \otimes \mathcal{R}$ (using orthogonality of $|\phi_0\rangle$ and $|\phi_1\rangle$) given by

$$\sigma = \frac{p_0}{p_0 + \frac{p_1}{2}}|\Omega_0\rangle\langle\Omega_0| + \frac{\frac{p_1}{2}}{p_0 + \frac{p_1}{2}}|\Omega_1\rangle\langle\Omega_1|$$

Let $T_0(\xi)$ be the probability that a state $\xi \in \mathcal{S}_2 \otimes \cdots \otimes \mathcal{S}_{k+1} \otimes \mathcal{R}$ passes all swap tests in $\mathcal{S}_2 \otimes \cdots \otimes \mathcal{S}_{k+1}$ with $|\phi_0\rangle$. We include the space $\mathcal{R}$ for convenience

only: notice that the choice of purification in the space $\mathcal{R}$ has no effect on this probability. Using this notation, we have

$$\begin{aligned}\Pr[\rho_0 \text{ passes Test 0}] &= (p_0 + \frac{p_1}{2}) \cdot \left(\frac{p_0}{p_0 + \frac{p_1}{2}} T_0(|\Omega_0\rangle\langle\Omega_0|) + \frac{\frac{p_1}{2}}{p_0 + \frac{p_1}{2}} T_0(|\Omega_1\rangle\langle\Omega_1|) \right) \\ &= p_0 T_0(|\Omega_0\rangle\langle\Omega_0|) + \frac{p_1}{2} T_0(|\Omega_1\rangle\langle\Omega_1|)\end{aligned}$$

Similarly, we define $T_1(\xi)$ for any ξ and we have

$$\Pr[\rho_1 \text{ passes Test 1}] = \frac{q_0}{2} T_1(|\Gamma_0\rangle\langle\Gamma_0|) + q_1 T_1(|\Gamma_1\rangle\langle\Gamma_1|)$$

which gives us

$$\begin{aligned}P &= \frac{1}{2} \left(\Pr[\rho_0 \text{ passes Test 0}] + \Pr[\rho_1 \text{ passes Test 1}] \right) \\ &= \frac{1}{2} \left(p_0 T_0(|\Omega_0\rangle\langle\Omega_0|) + \frac{p_1}{2} T_0(|\Omega_1\rangle\langle\Omega_1|) + \frac{q_0}{2} T_1(|\Gamma_0\rangle\langle\Gamma_0|) + q_1 T_1(|\Omega_1\rangle\langle\Omega_1|) \right)\end{aligned} \tag{9.4}$$

Consider the states $\xi_0 = p_0|\Omega_0\rangle\langle\Omega_0| + p_1|\Omega_1\rangle\langle\Omega_1|$ and $\xi_1 = q_0|\Gamma_0\rangle\langle\Gamma_0| + q_1|\Gamma_1\rangle\langle\Gamma_1|$. These states are obtained from ρ_0 and ρ_1 by discarding the system in $\mathcal{S}_1$. This implies that they have the properties in the statement of the Lemma, i.e. the reduced states of ξ_0 and x_1 on $\mathcal{A}_2 \otimes \cdots \otimes \mathcal{A}_{k+1}$ are equal. Thus, by induction, we know that $\frac{1}{2}(T_0(\xi_0) + T_1(\xi_1)) \leq \frac{1}{2} + \frac{1}{2^{k+1}}$. This means that:

$$\frac{1}{2} \left(p_0 T_0(|\Omega_0\rangle\langle\Omega_0|) + p_1 T_0(|\Omega_1\rangle\langle\Omega_1|) + q_0 T_1(|\Gamma_0\rangle\langle\Gamma_0|) + q_1 T_1(|\Gamma_1\rangle\langle\Gamma_1|) \right) \leq \frac{1}{2} + \frac{1}{2^{k+1}}$$

Using this, as well as Equation (9.4), we have

$$\begin{aligned}P &= \frac{1}{2} \left(p_0 T_0(|\Omega_0\rangle\langle\Omega_0|) + \frac{p_1}{2} T_0(|\Omega_1\rangle\langle\Omega_1|) + \frac{q_0}{2} T_1(|\Gamma_0\rangle\langle\Gamma_0|) + q_1 T_1(|\Gamma_1\rangle\langle\Gamma_1|) \right) \\ &= \frac{1}{4} + \frac{1}{2^{k+2}} + \frac{p_0}{4} T_0(|\Omega_0\rangle\langle\Omega_0|) + \frac{q_1}{4} T_1(|\Gamma_1\rangle\langle\Gamma_1|) \\ &\leq \frac{1}{2} + \frac{1}{2^{k+2}},\end{aligned}$$

where the final inequality is by Equation (9.3). ■

Proof: [Proof of Lemma 13] For simplicity, let $\rho_i = \mathrm{tr}_{\mathcal{B}} |\phi_i\rangle\langle\phi_i|$. We have

$$2 - \varepsilon \leq \| \rho_0 - \rho_1 \|_{\mathrm{tr}} = \mathrm{tr} |\rho_0 - \rho_1| = \mathrm{tr}\, \Pi_+(\rho_0 - \rho_1) - \mathrm{tr}\, \Pi_-(\rho_0 - \rho_1), \tag{9.5}$$

where Π_+ and Π_- are the projectors onto the positive and negative eigenspaces of $\rho_0 - \rho_1$ respectively. Notice that

$$\mathrm{tr}(\Pi_+ \rho_0) = \mathrm{tr}(\Pi_+(\rho_0 - \rho_1)) + \mathrm{tr}(\Pi_+ \rho_1) \geq \mathrm{tr}(\Pi_+(\rho_0 - \rho_1)),$$

and similarly $\mathrm{tr}(\Pi_- \rho_1) \geq -\mathrm{tr}(\Pi_-(\rho_0 - \rho_1))$, which implies that

$$\mathrm{tr}(\Pi_+ \rho_0) + \mathrm{tr}(\Pi_- \rho_1) \geq \mathrm{tr}(\Pi_+(\rho_0 - \rho_1)) - \mathrm{tr}(\Pi_-(\rho_0 - \rho_1)) \geq 2 - \varepsilon,$$

by Equation (9.5). This implies that $\mathrm{tr}(\Pi_+ \rho_0) \geq 1 - \varepsilon$ and $\mathrm{tr}(\Pi_- \rho_1) \geq 1 - \varepsilon$.

We introduce the states ρ_i' given by the (renormalized) projection of ρ_0 and ρ_1 into the spaces spanned by Π_+ and Π_-, respectively. Since these are orthogonal projectors the states ρ_0' and ρ_1' are orthogonal. Notice also that

$$\| \rho_0 - \rho_0' \|_{\mathrm{tr}} = \mathrm{tr}\,|\rho_0 - \rho_0'| = \mathrm{tr}(\Gamma_+(\rho_0 - \rho_0')) - \mathrm{tr}(\Gamma_-(\rho_0 - \rho_0')) = 2\,\mathrm{tr}(\Gamma_+(\rho_0 - \rho_0')),$$

where Γ_+, Γ_- are the projectors onto the positive and negative eigenspaces of $\rho_0 - \rho_0'$, and we have also used the fact that $\mathrm{tr}(\rho_0 - \rho_0') = 0$, which implies that the positive portion of $\rho_0 - \rho_0'$ has the same trace as the negative portion. Consider the positive eigenspace of $\rho_0 - \rho_0'$. This is precisely the subspace spanned by the support of ρ_0 that lies outside the support of ρ_0', i.e. this is exactly the space spanned by the projector $\Pi_- = \Gamma_+$. Using this observation

$$\| \rho_0 - \rho_0' \|_{\mathrm{tr}} = 2\,\mathrm{tr}(\Gamma_+(\rho_0 - \rho_0')) = 2\,\mathrm{tr}(\Pi_- \rho_0) \leq 2\varepsilon, \tag{9.6}$$

where we have used the fact that $\mathrm{tr}(\Pi_- \rho_0) = 1 - \mathrm{tr}(\Pi_+ \rho_0) \leq \varepsilon$. A similar argument establishes the fact that

$$\| \rho_1 - \rho_1' \|_{\mathrm{tr}} = 2\,\mathrm{tr}(\Pi_+ \rho_1) \leq 2\varepsilon. \tag{9.7}$$

Finally, we note that Equations (9.6) and (9.7) and Uhlmann's theorem imply that there exist purifications $|\phi_0'\rangle, |\phi_1'\rangle \in \mathcal{A} \otimes \mathcal{B}$ of ρ_0' and ρ_1' such that

$$\langle \phi_i' | \phi_i \rangle = \mathrm{F}(\rho_i', \rho_i) \geq 1 - \varepsilon.$$

This, combined with the orthogonality of ρ_0' and ρ_1', completes the proof. ■

Notice that in the original bit commitment protocol the Receiver applies the swap test to $|\phi^*\rangle|0\rangle$ and the output of $(U_b^\dagger \otimes \mathbb{1})(\sigma_b)(U_b \otimes \mathbb{1})$ where σ_b is the state sent during the protocol. Since $U_b^\dagger$ is unitary, this is equivalent to applying the swap test between σ_b and the state $|\phi_b\rangle = (U_b \otimes \mathbb{1})|\phi^*\rangle|0\rangle$, for whatever value of b the Sender has revealed. Viewed in this way, the receiver applies the swap test between σ_b and one of two *almost* orthogonal states. Furthermore, these two states have the property that the reduced states on the space $\mathcal{O}$ have negligible fidelity. Notice also that the Sender may send one of two states σ_0 and σ_1 depending on the value that he wishes to reveal. Since we are interested in the sum of the probabilities that the Sender can successfully reveal both 0 and 1 in a given instance of the protocol, we may assume that the first message stays the same, i.e. that $\mathrm{tr}_{\mathcal{G}}\,\sigma_0 = \mathrm{tr}_{\mathcal{G}}\,\sigma_1$. This is exactly the condition in Lemma 12 with the exception that instead of the orthogonality of the states $|\phi_i\rangle$ we have only approximate orthogonality. We are able to overcome this obstacle with the following Lemma.

Lemma 13 *Let $|\phi_0\rangle, |\phi_1\rangle \in \mathcal{A} \otimes \mathcal{B}$ such that $\| \mathrm{tr}_{\mathcal{B}}\,|\phi_0\rangle\langle\phi_0|, \mathrm{tr}_{\mathcal{B}}\,|\phi_1\rangle\langle\phi_1| \|_{\mathrm{tr}} \geq 2 - \varepsilon$. Then there exist states $|\phi_0'\rangle, |\phi_1'\rangle \in \mathcal{A} \otimes \mathcal{B}$ such that*

1. *$\langle \phi_i' | \phi_i \rangle \geq 1 - \varepsilon$ for $i \in \{0, 1\}$,*
2. *$\mathrm{tr}_{\mathcal{B}}\,|\phi_0'\rangle\langle\phi_0'|$ and $\mathrm{tr}_{\mathcal{B}}\,|\phi_1'\rangle\langle\phi_1'|$ are orthogonal.*

This Lemma shows that we may replace the two states that are almost orthogonal with nearby states that have exactly the orthogonality property required by Lemma 12, which we can in turn use to show that the protocol

repeated k times is statistically binding. To do so, notice that the two states $|\phi_0\rangle$ and $|\phi_1\rangle$, which are given by applying the circuits Q_0 and Q_1 to the state $|\phi^*\rangle|0\rangle$, satisfy

$$\begin{aligned} \| \, |\phi_0\rangle\langle\phi_0| - |\phi_1\rangle\langle\phi_1| \, \|_{\mathrm{tr}} &\geq \| \, \mathrm{tr}_{\mathcal{G}}(|\phi_0\rangle\langle\phi_0| - |\phi_1\rangle\langle\phi_1|) \, \|_{\mathrm{tr}} \\ &= \| \, ((Q_0 - Q_1) \otimes I)(|\psi^*\rangle\langle\psi^*|) \, \|_{\mathrm{tr}} \\ &= \| \, Q_0 - Q_1 \, \|_{\diamond} \\ &\geq 2 - \mu(n), \end{aligned}$$

These states are not orthogonal, but are nearly so. We may, however, use Lemma 13 to obtain $|\phi_0'\rangle$ and $|\phi_1'\rangle$ that have the orthogonality property required by Lemma 12 that have inner product at least $1 - \mu(n)$ with the original states $|\phi_0\rangle$ and $|\phi_1\rangle$, respectively.

We now relate the probability that the state ρ passes our Test 0, i.e. the k swap tests with the state $|\phi_0\rangle^{\otimes k}$ to the probability that the same state ρ passes the k swap tests with the state $|\phi_0'\rangle^{\otimes k}$ (denoted by Test$'$ 0). The difference of these probabilities is upper bounded by the trace distance of the difference of the states $|\phi_0\rangle^{\otimes k}$ and $|\phi_0'\rangle^{\otimes k}$, since we can view the swap test with ρ as a measurement to distinguish these two states. This gives

$$\begin{aligned} |\Pr[\rho \text{ passes Test } 0] - \Pr[\rho \text{ passes Test}' \, 0]| &\leq \| \, (|\phi_0\rangle\langle\phi_0|)^{\otimes k} - (|\phi_0'\rangle\langle\phi_0'|)^{\otimes k} \, \|_{\mathrm{tr}} \\ &= 2\sqrt{1 - |\langle\phi_0'|\phi_0\rangle|^{2k}} \\ &\leq 2\sqrt{1 - (1 - \mu(n))^{2k}} \\ &\leq 2\sqrt{2k\mu(n)}, \end{aligned}$$

where the final inequality is Bernoulli's inequality. Similarly we have

$$|\Pr[\rho \text{ passes Test } 1] - \Pr[\rho \text{ passes Test}' \, 1]| \leq 2\sqrt{2k\mu(n)}$$

Hence, for the binding property of our scheme we have

$$\begin{aligned} &\frac{1}{2}\left(\Pr[\rho \text{ passes Test } 0] + \Pr[\rho \text{ passes Test } 1]\right) \\ &\quad\leq \frac{1}{2}\left(\Pr[\rho \text{ passes Test}' \, 0] + \Pr[\rho \text{ passes Test}' \, 1]\right) + 2\sqrt{2k\mu(n)} \\ &\quad\leq \frac{1}{2} + \frac{1}{2^{k+1}} + 2\sqrt{2k\mu(n)}. \end{aligned}$$

since, for the Test$'$ 0 and Test$'$ 1 we can use Lemma 12 for the perfect case. This quantity is negligibly larger than $1/2$, as we may take k any polynomial and μ is a negligible function. ■

The proposition gives the desired result ■

9.4 Quantum (b_c, h_s)-commitments unless QIP $\subseteq$ QMA

Theorem 17 *If* QIP $\not\subseteq$ QMA*, then there exists a non-interactive auxiliary-input quantum (b_c, h_s)-commitment scheme with quantum advice on an infinite set I.*

Proof: Recall the Complete problem $\Pi = \{\Pi_Y, \Pi_N\}$ from Definition 19 with inputs the mixed-state circuits (Q^0, Q^1) from $\mathbf{D}(\mathcal{X} \otimes \mathcal{Y})$ to a single bit and $n = |(Q^0, Q^1)|$. To show this Theorem, we first show the following Lemma

Lemma 14 *If* QIP $\not\subseteq$ QMA*, there exist two auxiliary-input superoperator ensembles* $\{Q^0\}_{(Q^0,Q^1)\in I}$ *and* $\{Q^1\}_{(Q^0,Q^1)\in I}$ *that are quantum computationally unwitnessable on an infinite set* I*.*

Proof: Let us consider the set Π_Y and suppose for contradiction that the two auxiliary-input superoperator ensembles $\{Q^0\}_{(Q^0,Q^1)\in\Pi_Y}$ and $\{Q^1\}_{(Q^0,Q^1)\in\Pi_Y}$ are quantum computationally witnessable, i.e. there exist polynomials (s, k, p) such that for all $(Q^0, Q^1) \in \Pi_Y$ the superoperators Q^0 and Q^1 are (s(n),k(n),p(n))-witnessable. In other words, there exist polynomials (s, k, p) such that for all $(Q^0, Q^1) \in \Pi_Y$ there exist two input states $\rho^0, \rho^1 \in \mathbf{L}(\mathcal{X} \otimes \mathcal{Y})$ such that first, there exists a state $\sigma \in \mathbf{L}(\mathcal{W})$ with $|\mathcal{W}| = k$ and an admissible superoperator $\Psi : \mathbf{L}(\mathcal{W} \otimes \mathcal{X}) \to \mathbf{L}(\mathcal{X})$ of size s, such that $\rho^1 = (\Psi \otimes \mathbb{1}_{\mathcal{Y}})(\sigma \otimes \rho^0)$; and second

$$\frac{1}{2}\left(\Pr[Q^0(\rho^0) = 1] + \Pr[Q^1(\rho^1) = 1]\right) \geq 1/2 + \frac{1}{p(n)}$$

Then, we provide a QMA protocol for the problem Π. Merlin sends ρ^0, σ (of size $k(n)$) and the classical description of Ψ (of size $s(n)$). Arthur with probability $1/2$ applies Q^0 on ρ^0 and accepts if he gets 1; and with probability $1/2$ he first creates ρ^1 from ρ^0, Ψ and σ, then applies Q^1 on it and also accepts if he gets 1.
(*Completeness*) If $(Q^0, Q^1) \in \Pi_Y$, we have

$$\Pr[\text{Arthur accepts}] = \frac{1}{2}\left(\Pr[Q^0(\rho^0) = 1] + \Pr[Q^1(\rho^1) = 1]\right) \geq \frac{1}{2} + \frac{1}{p(n)}$$

(*Soundness*) If $(Q^0, Q^1) \in \Pi_N$, then for any cheating Merlin, Arthur receives a state ρ^0_*, form which he constructs (with half probability) a state ρ^1_* each in space $\mathcal{X} \otimes \mathcal{Y}$ such that $\mathrm{tr}_{\mathcal{X}}\, \rho^0_* = \mathrm{tr}_{\mathcal{X}}\, \rho^1_*$. By definition of Π_N, we have

$$\Pr[\text{Arthur accepts}] = \frac{1}{2}\left(\Pr[Q^0(\rho^0_*) = 1] + \Pr[Q^1(\rho^1_*) = 1]\right) = \frac{1}{2} + \mu(n)$$

We have an inverse polynomial gap between completeness and soundness and hence we conclude that $\Pi \in$ QMA. This proves that there is an nonempty I that satisfies the property of our Lemma. Note that if I is finite, then by hard-wiring this finite number of instances into the QMA verifier (who always accepts these instances), we have again that QIP $\subseteq$ QMA. So if QIP $\not\subseteq$ QMA then the above I is infinite. ■

To finish the proof of the Theorem, we now need to show the following

Lemma 15 *The two auxiliary-input superoperator ensembles* $\{Q^0\}_{(Q^0,Q^1)\in I}$ *and* $\{Q^1\}_{(Q^0,Q^1)\in I}$ *that are quantum computationally unwitnessable on the infinite set* $I \subseteq \Pi_Y$ *imply a non-interactive quantum* (b_c, h_s)*-commitment scheme with quantum advice on* I*.*

Proof: *Commitment scheme* For each $(Q^0, Q^1) \in I \subseteq \Pi_Y$, we consider the following commitment scheme

- Let $n = |(Q^0, Q^1)|$ be the security parameter. The sender receives as quantum advice ρ^0, ρ^1, with each ρ^i in space $\mathcal{X}^i \otimes \mathcal{Y}^i$ such that:

  1. $\mathrm{tr}_{\mathcal{X}}\, \rho^0 = \mathrm{tr}_{\mathcal{X}}\, \rho^1$
  2. $\frac{1}{2}\left(\Pr[Q^0(\rho^0) = 1] + \Pr[Q^1(\rho^1) = 1]\right) \geq 1 - \mu(n)$

  For consistency with our definitions, we also suppose that the Receiver gets a copy of ρ^0, ρ^1. These states will not be used in the honest case and moreover they will not harm the security for a cheating Receiver.

- (Commit phase) To commit to bit b, the Sender sends the state in register $\mathcal{Y}^b$ to the Receiver.

- (Reveal phase) To reveal b, the Sender sends the state in register $\mathcal{X}^b$. The Receiver applies Q^b on the space $\mathcal{X}^b \otimes \mathcal{Y}^b$ and accepts if he gets 1.

Statistical hiding property The states that the receiver gets in the commit phase satisfy $\mathrm{tr}_{\mathcal{X}}\, \rho^0 = \mathrm{tr}_{\mathcal{X}}\, \rho^1$ and hence our scheme is perfectly hiding.
Computationally binding property The property follows from the fact that the two auxiliary-input superoperator ensembles $\{Q^0\}_{(Q^0,Q^1)\in I}$ and $\{Q^1\}_{(Q^0,Q^1)\in I}$ are quantum computationally unwitnessable. Let us fix $(Q^0, Q^1) \in I$ with $|(Q^0, Q^1)| = n$. After the reveal phase, the Receiver has a state ρ_*^b in space $\mathcal{X} \otimes \mathcal{Y}$, where b is the revealed bit. Since we consider dishonest senders $S^*_{(Q^0,Q^1)}$ that are quantum polynomial time machines with quantum advice, the states ρ_*^0 and ρ_*^1 satisfy the property 2 of Definition 27. Hence, for all but finitely many $(Q^0, Q^1) \in I$ they must not satisfy property 1 of Definition 27. Then, for such $(Q^0, Q^1) \in I$ we have

$$\begin{aligned} P_{S^*_{(Q^0,Q^1)}} &= \frac{1}{2}\left(\Pr[S^*_{(Q^0,Q^1)} \text{ reveals } b = 0] + \Pr[S^*_{(Q^0,Q^1)} \text{ reveals } b = 1]\right) \\ &= \frac{1}{2}\left(\Pr[Q_0(\rho_*^0) = 1] + \Pr[Q_1(\rho_*^1) = 1]\right) \\ &\leq \frac{1}{2} + \frac{1}{p(n)} \end{aligned}$$

for all polynomials p. ■

From the above two Lemmata, we conclude that unless $\mathsf{QIP} \subseteq \mathsf{QMA}$ there exists a non-interactive auxiliary-input quantum (b_c, h_s)-commitment scheme with quantum advice on infinite set I. ■

This result, combined with Theorem 16 and Proposition 25, completes the proof of Theorem 12.

Chapter 10

Conclusions

In this thesis, we presented a study of two-party quantum cryptographic primitives in the information theoretic setting. We considered basic quantum cryptographic primitives as a way of understanding what is possible and what is impossible in a quantum world. Since the impossibility of quantum coin flipping and quantum bit commitment can explain many features of quantum physics, we first wanted to quantify to what extent these cryptographic primitives are impossible. In the first part of this thesis, we showed tight bounds for both quantum coin flipping ($\frac{1}{\sqrt{2}}$ bound) and quantum bit commitment (0.739 bound)

These bounds raise interesting questions. For example, following the line of thought of Smolin,Fuchs and Brassard [FM01, Bra05], one could ask the following question

How can we characterize theories that:

1. *Allow key distribution*
2. *Allow coin flipping up to cheating probabilities of* $\frac{1}{\sqrt{2}}$
3. *Allow bit commitment up to cheating probabilities of* 0.739

At the end of the first part, we also tried to extend these bounds for quantum oblivious transfer. We derived the bounds for quantum bit commitment to obtain - unfortunately not tight - bounds for quantum oblivious transfer. Reducing oblivious transfer to quantum bit commitment presents the following underlying question

If I can get some information about a bit x_0 *and I can get some information about a bit* x_1*, what information can I get about the two bits* (x_0, x_1) *?*

The Learning in Sequence Lemma that we showed in Chapter 6 partially answers this question by stating that if someone can guess bit x_0 with probability $\cos^2(\alpha_0)$ and x_1 with probability $\cos^2(\alpha_1)$ then he can learn both with probability at least $\left(\frac{\cos^2(\alpha_0)+\cos^2(\alpha_1)}{2}\right)\cos^2(\alpha_0+\alpha_1)$. This is in sharp contrast with the classical case where we know that one can learn both bits with probability at least $\cos^2(\alpha_0)\cos^2(\alpha_1)$ which is much higher than our quantum bound. Even if we only show lower bounds for the learning of (x_0, x_1), we can construct some

examples where the probability of learning both bits is strictly smaller than $\cos^2(\alpha_0)\cos^2(\alpha_1)$ when information about x_0 and x_1 is encoded into a quantum state. This also seems to be a fundamental characteristic of quantum mechanics as a carrier of classical information. In future work, we plan to extend this study and show how such learning lemmata are related to quantum non-locality.

We then tried to base quantum cryptographic primitives solely on quantum non-locality. In this setting, we showed that Alice and Bob can use a quantum state to perform cryptographic tasks even without trusting their quantum apparatus and without trusting each other. This is in contrast with quantum key distribution based on non-locality where Alice and Bob cooperate against a third party, Eve. It is a new application of non-locality and it is interesting that quantum non-locality can be used even without the cooperation of two honest parties.

One important thing to notice is that we do not obtain the same bounds in this setting as in the general setting. The question that arises from this is

Can we build optimal quantum coin flipping and quantum bit commitment protocols that rely only on the violation of Bell's inequalities ?

We then presented a quantum coin flipping protocol that was tolerant to losses. Even if the obtained protocol cannot be used for practical applications because of the high bias, the methods we used to deal with losses are efficient and generic and we feel that this method can be used for many other protocols.

The remaining question is to find similar techniques against quantum noise. It is relatively easy to deal with noise when Alice and Bob cooperate against a third party or if one of the players is physically bounded. However, there are no methods to deal with noise in the most general case. It is not a priori clear whether dealing with noise in the general setting is even possible with good parameters.

Finally, we showed under what conditions computational bit commitment was possible. We extended classical relationships between bit commitment and zero-knowledge protocols to the quantum case. We showed how the complete problem for quantum zero-knowledge protocols and the ability to solve it in QMA is related to the existence of quantum bit commitment schemes.

It will be instructive to get a better understanding of quantum zero-knowledge protocols and quantum Merlin-Arthur protocols. If we find some notable difference in these quantum classes compared to their classical counterparts, it might be possible to construct quantum computational commitments from weak computational assumptions.

Bibliography

[Aar11] Scott Aaronson. Impossibility of succinct quantum proofs for collision-freeness. arxiv, quant-ph: 1101.0403, 2011.

[ABDR04] Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Rohrig. Multiparty quantum coin flipping. In *CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259, Washington, DC, USA, 2004. IEEE Computer Society.

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98(23):230501, Jun 2007.

[AGM06] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 97(12):120405, Sep 2006.

[Amb01] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. In *STOC '01: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, Washington, DC, USA, 2001. IEEE Computer Society.

[AMS10] N. Aharon, S. Massar, and J. Silman. A family of loss-tolerant quantum coin flipping protocols. 2010. quant-ph:0711.4114.

[ATVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 705–714, New York, NY, USA, 2000. ACM.

[BB84] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. in Proc. Of IEEE Inter. Conf. on Computer Systems and Signal Processing, Bangalore, Kartarna, (Institute of Electrical and Electronics Engineers, New York, 1984.

[BBBG08] Guido Berlin, Gilles Brassard, Felix Bussieres, and Nicolas Godbout. Loss-tolerant quantum coin flipping. In *ICQNM '08: Proceedings of the Second International Conference on Quantum, Nano and Micro Technologies (ICQNM 2008)*, pages 1–9, Washington, DC, USA, 2008. IEEE Computer Society.

[BGG+90] Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Håstad, Joe Kilian, Silvio Micali, and Phillip Rogaway. Everything provable is provable in zero-knowledge. In *Proceedings of Advances in Cryptology (CRYPTO) 1988*, volume 403 of *Lecture Notes in Computer Science*, pages 37–56, 1990.

[BHK05] J. Barrett, L. Hardy, and A. Kent. No Signaling and Quantum Key Distribution. *Physical Review Letters*, 95(1):010503–+, June 2005.

[BLM+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71(2):022101, Feb 2005.

[BLM+09] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani. Device-independent state estimation based on bell's inequalities. *Phys. Rev. A*, 80(6):062327, Dec 2009.

[Blu81] Manuel Blum. Coin flipping by telephone. In *CRYPTO*, pages 11–15, 1981.

[BM04] Jonathan Barrett and Serge Massar. Security of quantum bit-string generation. *Phys. Rev. A*, 70(5):052310, Nov 2004.

[Bra05] G. Brassard. Is information the key? *Nature Physics. v1. 2-4*, 2005.

[Cha10] André Chailloux. Improved loss-tolerant quantum coin flipping. *AQIS'10*, 2010.

[CK09] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. *Foundations of Computer Science (FOCS)*, pages 527–533, 2009.

[CK11] André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. *Foundations of Computer Science (FOCS)*, 2011.

[CKR11] A. Chailloux, I. Kerenidis, and B. Rosgen. Quantum Commitments from Complexity Assumptions. *ICALP'11*, October 2011.

[CKS10] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for Quantum Oblivious Transfer. In Kamal Lodaya and Meena Mahajan, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)*, volume 8 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 157–168, Dagstuhl, Germany, 2010. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[CLS01] Claude Crépeau, Frédéric Légaré, and Louis Salvail. How to convert the flavor of a quantum bit commitment. In *Proceedings of EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 60–77, 2001.

[Col09] R. Colbeck. Quantum And Relativistic Protocols For Secure Multi-Party Computation. *ArXiv e-prints*, November 2009.

[Cré87] Claude Crépeau. Equivalence between two flavours of oblivious transfer. In *Advances in Cryptology: CRYPTO '87*, 1987.

[DFR+07] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Proceedings of the 27th annual international cryptology conference on Advances in cryptology*, CRYPTO'07, pages 360–378, Berlin, Heidelberg, 2007. Springer-Verlag.

[DKSW07] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: the possible and the impossible. *Physical Review A*, 76:032328, 2007.

[DW09] Andrew Drucker and Ronald de Wolf. Quantum proofs for classical theorems, 2009.

[EGL82] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology: Proceedings of CRYPTO 82*, 1982.

[Eke91] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, Aug 1991.

[Fey82] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6&7):467–488, 1982.

[FG99] Christopher A. Fuchs and Jeroen Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inform. Theory 45. No*, pages 45–1216, 1999.

[FM01] Christopher A. Fuchs and N. David Mermin. *Notes on a Paulian Idea: Foundational, Historical, Anecdotal and Forward-Looking Thoughts on the Quantum.* 2001. cite arxiv:quant-ph/0105039 Comment: 504 pages including introduction, table of contents, and index of names; no figures.

[GHZ89] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going Beyond Bell's Theorem. 1989.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3), 1991.

[Gro97] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack, 1997.

[Hel67] C. W. Helstrom. Detection theory and quantum mechanics. *Information and Control*, 10(3):254–291, 1967.

[JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. In *Proceedings of the 42nd ACM Symposium on the Theory of Computing*, 2010.

[JKP09] Nathaniel Johnston, David W. Kribs, and Vern I. Paulsen. Computing stabilized norms for quantum operations via the theory of completely bounded maps. *Quantum Information and Computation*, 9(1&2):16–35, 2009.

[Ken99a] Adrian Kent. Coin tossing is strictly weaker than bit commitment. *Phys. Rev. Lett.*, 83(25):5382–5384, Dec 1999.

[Ken99b] Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83(7):1447–1450, Aug 1999.

[Kit97] A. Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[Kit03] A Kitaev. Quantum coin-flipping. presentation at the 6th workshop on quantum information processing (qip 2003), 2003.

[KN04] I. Kerenidis and A. Nayak. Weak coin flipping with small bias. *Inf. Process. Lett.*, 89(3):131–135, 2004.

[Kob07] Hirotada Kobayashi. General Properties of Quantum Zero-Knowledge Proofs. *ArXiv Quantum Physics e-prints*, quant-ph/0705.1129, May 2007.

[KSV02] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[KvM02] Adam R. Klivans and Dieter van Melkebeek. Graph Nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31(5):1501–1526, 2002.

[KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd ACM Symposium on the Theory of Computing*, pages 608–617, 2000.

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17):3410–3413, Apr 1997.

[LWW+10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686–689, October 2010.

[Mas09] Lluís Masanes. Universally composable privacy amplification from causality constraints. *Phys. Rev. Lett.*, 102(14):140501, Apr 2009.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, Apr 1997.

[Mer90] N. David Mermin. What's wrong with these elements of reality? *Physics Today*, 43(6):9–11, 1990.

[MMMO06] Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In *ICALP (1)*, pages 72–83, 2006.

[Moc04] Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *FOCS '04: Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 2–11, Washington, DC, USA, 2004. IEEE Computer Society.

[Moc05] C. Mochon. Large family of quantum weak coin-flipping protocols. *Phys. Rev. A*, 72(2):022341–+, August 2005.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias, 2007. quant-ph:0711.4114.

[MV06] Peter Bro Miltersen and N. V. Vinodchandran. Derandomizing Arthur-Merlin games using hitting sets. *Computational Complexity*, 14(3):256–279, 2006.

[MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[MY03] D. Mayers and A. Yao. Self testing quantum apparatus. *ArXiv Quantum Physics e-prints*, July 2003.

[Nay99] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:369, 1999.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[NS03] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67(1):012304, 2003.

[OW93] Rafail Ostrovsky and Avi Wigderson. One-way functions are essential for non-trivial zero-knowledge. In *Proceedings of the 2nd Israel Symposium on Theory and Computing Systems*, pages 3–17, 1993.

[PAM+10] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, April 2010.

[Pau02] Vern Paulsen. *Completely Bounded Maps and Operator Algebras*, volume 78 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2002.

[Rab81] Michael Rabin. How to exchange secrets by oblivious transfer. In *Technical Report TR-81, Aiken Computation Laboratory, Harvard University*, 1981.

[RW05] Bill Rosgen and John Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Proceedings of the 20th Conference on Computational Complexity*, pages 344–354, 2005.

[SCA+11] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully Distrustful Quantum Cryptography. *Physical Review Letters*, 2011.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Smi83] R. R. Smith. Completely bounded maps between C*-algebras. *Journal of the London Mathematical Society*, s2-27(1):157, 1983.

[SR01] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(1):012310, 2001.

[SSS09] Louis Salvail, Christian Schaffner, and Miroslava Sotakova. On the power of two-party quantum cryptography. In *ASIACRYPT 2009*, 2009.

[Vad99] Salil Pravin Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, 1999. Supervisor-Shafi Goldwasser.

[Vad06] Salil Vadhan. An unconditional study of computational zero knowledge. *SIAM Journal on Computing*, 36(4):1160–1214, 2006.

[Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, pages 537 – 546, 2000.

[Wat02] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science*, pages 459 – 468, 2002.

[Wat03] John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

[XQL10] F. Xu, B. Qi, and H.-K. Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11), November 2010.