Quantum Primitives for Secure Two-party Computations and Entanglement Attacks

Minh-Dung Dang

Quantum Primitives for Secure Two-party Computations and Entanglement Attacks

by Minh-Dung Dang

Dissertation
submitted in partial fulfillment of the requirements for the degree of

Docteur
de TELECOM ParisTech

Spécialité : Informatique et Réseaux

TELECOM ParisTech
Network and Computer Sciences Department
Paris, France

2008

Dedicated to

my Parents, my Sister, and my Friends!

Quantum Primitives for Secure Two-party Computations and Entanglement Attacks

by

Minh-Dung Dang

B. S., Hanoi University of Technology, 2001
M. S., Institut de la Francophonie pour l'Informatique, 2003

ABSTRACT

In this thesis, we are interested in the theory of unconditional secure two-party computations. The primitives of Oblivious Transfer (OT) and Bit Commitment (BC) are fundamental in the design of these cryptographic applications. The principal object of this thesis relates to the theory of the design of unconditional secure OT and BC.

On one hand, my works are inspired from the framework of design of oblivious transfer from noisy communication channels, pioneered by Crépeau, Morozov et al. [Cré97, CMW04]. The principle of this framework is to conceive, from the noisy channels, an intermediate erasure model, the Binary Symmetric Erasure Channel, which is a variant of oblivious transfer. We contributed to this framework by proposing a more general intermediate model, the Binary Symmetric Multi-Error-Rate Channel, which also can be built from almost noisy channels. With this intermediate model, we can build a protocol of oblivious transfer from the noisy channels more effectively.

In addition, inspired from the motivating works of building noisy channel for oblivious transfer from Wiesner's quantum conjugate coding (QCC) [BBC$^+$93, Cré94], we expose a case study on emulating noisy model by a quantum nonorthogonal coding (QNOC) scheme which uses two non-orthogonal pure state for encoding two values of the classical bit. We show that QNOC is equivalent to QCC, and can only implement semi-honest oblivious transfer. We also show that the implementation of oblivious transfer from QNOC can be secure if we have access to a secure bit commitment protocol. An attempt to secure the implementation based on a coin flipping protocol is shown to be impossible by attacks using quantum entanglement.

On the other hand, this research are inspired from the no-go theorems of Mayers, Lo and Chau on the implementation of oblivious transfer and bit commitment in the framework of quantum information [May97, LC97, Lo97]. However the theorems has been being only interpreted in a pure quantum two-party model, and caused controversial discussions.

We revise the quantum model for general two-party protocols concerning classical and quantum computation and communication. We state that in the general model, a classical channel is inevitably macroscopic and its decoherence is so strong that quantum information is not accepted to be transfered on it. Thus, the quantum model for two-party protocols becomes *three-party*, consisted of three physical components: the machine of Alice, the machine of

Bob, and the environment coupled with the macroscopic channel which should measure the classical messages.

One should then reconsider the no-go theorems in this general model. Indeed, with the faithful interpretation of general protocols in this three-party model, we reaffirm that these two-party protocols cannot implement unconditionally secure oblivious transfer and bit commitment.

Inspired from this three-party model, penalized by the no-go theorems, we can go further to apply these negative results to the protocols using quantum trusted third-parties, named *two-party oracles*, which either do not store information entangled with information in Alice's and Bob's machines, or only make redundant copies of public information of Alice and Bob. We see that this extended no-go result cover Kent statement on coin-flipping based protocols [Ken99], as with the model of *two-party oracle*, one can easily implement a protocol of coin flipping.

Moreover, this extension implies a corollary which relates to the thermodynamics: implementations of unconditionally secure bit commitment, oblivious transfer, and in general two-party computation, require the erasure of information and thus a dissipation of heat to the external environment [Lan61].

ACKNOWLEDGMENTS

I express my deep gratitude to Patrick Bellot, my advisor, for having received me as a PhD student and for his invaluable encouragement throughout my PhD studies. He always spends time and enthusiasm for discussions with me. He appreciates any critical, even stupid, thought of mines. He is always a great professor and an ultimate friend.

Special thanks go to Nguyen-Vu Duong for his availability for help and support. His compliments have been encouraging me much. He always encourages me during the redaction of this thesis, and helps me for the proof-reading.

I am very grateful to Hong-Quang Nguyen, my co-advisor, for his support and discussions. He is always enthusiastic about sharing experiences to me.

I would like to thank Romain Alléaume for introducing me to the domain of quantum physics and quantum information.

I would like to thank Alain Maruani for his valuable encouragements and finally acceptating to participate in the jury of my PhD defense.

I am very thankful to the financial supporters of my PhD studies: l'Institut de la Francophonie pour l'Informatique (IFI) et l'Ecole Nationale Supérieure de Télécommunications de Paris (ENST).

I would thank the administrative and technical staffs at IFI and ENST for always being helpful, particularly Thi-Hong-Loan Nguyen, Hayette Soussou and Sophie Beranger.

I am deeply grateful to my friends for the beautiful time throughout my PhD studies, in particular the members of Chuoi and ChuoiFoot team: Hieu Mu, Thanh CD, Phuong Cap, Long PD, Son Toet, Minh Anh, Dao Ha (dai ca), Phuong Keu, Hai Khit, Tuan Noir, Manh DS, Tu Beo, QMinh, Linh Tuoi, Khanh Rau, ...

Very special thanks go to my colleagues at ENST, Tan-Nguyen Pham-Viet, Quoc-Cuong Le, Van-Tam Nguyen, Thi-Mai-Trang Nguyen, Huu-Quynh Nguyen, Xiaoyun Xue, Syed Naqvi, and the interns from IFI working at ENST.

I am deeply indebted to my parents and my family for encouraging me during my studies. Ultimately, this thesis is dedicated to my parents.

—Minh-Dung Dang
Ecole nationale superieure des
telecommunications de Paris

Contents

List of Figures

Summary in French

0.1 Introduction

La Cryptographie a été inventée pour cacher les informations durant une communication. Elle est restée plutôt un art qu'une science jusqu'à ce que Shannon montre comment prouver la sécurité d'un schéma de chiffrement en modélisant la quantité d'information révélée dans le modèle probabiliste de la Théorie de l'Information [Sha48, Sha49]. Ultérieurement, Diffie & Hellman ont introduit une autre notion de sécurité basée sur la complexité des calculs [DH76] : nous considérons que la sécurité est assurée si nous pouvons prouver que si l'adversaire arrive à casser le système alors c'est qu'il peut résoudre un problème "difficile". Une majorité d'applications cryptographiques de nos jour sont basées sur le système RSA dont la sécurisé est garantie par la complexité de la factorisation des grands nombres entiers.

Or, cette sécurisé calculatoire est basée sur des hypothèses non prouvées: l'hypothèse du modèle abstrait des machines à calcul, celui de la machine de Turing, et, également, des hypothèses sur les problèmes difficiles sur cette machine. La sécurité calculatoire est donc potentiellement menacée par la découverte d'algorithmes et de modèles avancés de calcul. Par exemple, la factorisation des grands nombres entiers deviendra facile si l'on peut construire un ordinateur quantique grâce à l'algorithme de Shor [Sho94]. En revanche, la sécurité basée sur la théorie de l'information de Shannon ne dépend pas des modèles de calcul et est appelée sécurité inconditionnelle. Malheureusement, dans le cadre de l'information classique, la construction des systèmes avec "sécurité inconditionnelle" n'est possible qu'avec des "hypothèses" sur des imperfections matérielles.

L'introduction de l'information quantique dans le domaine de la cryptographie a pour but de construire des schémas vraiment inconditionnellement sécurisés, en se reposant sur les lois de la physique quantique. La cryptographie quantique a démarrée avec les schémas d'échange de clés secrètes (QKD) d'une sécurité inconditionnelle [BB84].

Par ailleurs, pendant longtemps, la Cryptographie Classique n'avait été liée qu'au problème de la protection des communications entre deux parties contre l'interception d'une troisième partie malfaisante. Elle ne se limite qu'à la protection de l'intégrité et à l'authenticité des communications. L'introduction de la théorie de calcul au domaine de la cryptographie avec les schémas à clef publique, par Diffie & Hellman, a ouvert l'ère de la Cryptographie Moderne. Elle donne lieu à de nombreuses applications plus sophistiquées et plus intéressantes [Gol01, Gol04].

La recherche effectuée dans cette thèse se rapporte aux protocoles primitifs quantiques pour le calcul sécurisé à deux parties, un sous-domaine de la Cryptographie.

0.2 Préliminaires

0.2.1 Le Calcul Sécurisé à Deux Parties

Une application centrale de la Cryptographie Moderne se focalise sur le calcul distribué sécurisé à deux parties : deux partenaires méfiants, nommés Alice et Bob, veulent collaborer pour calculer une fonction sur leurs données mais chacun veut garder secrètes ses données privées à l'exception de ce que l'autre peut retirer à partir du résultat final de la fonction.

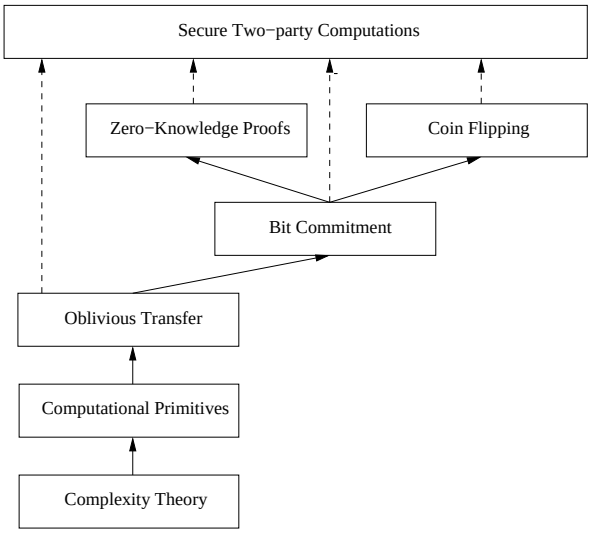

Figure 1: Fondations du calcul sécurisé à deux parties

De nombreuses contributions du domaine ont formé un cadre de travail générique pour cette application, avec des primitivess fondatrices :

- *Oblivious Transfer (OT)* : c'est un schéma de transmission asymétrique où l'émetteur envoie deux messages (deux bits) au récepteur qui peut choisir à lire un et seulement un des deux messages pendant que l'émetteur ignore le choix du récepteur.

  Ce schéma primitif sert à la construction des schémas d'évaluation "oblivious" pour les calculs sécurisés dans le modèle "semi-honest" où les utilisateurs respectent les conduites décrites par les protocoles.

- *Coin Flipping (CF)* : c'est le schéma pour que Alice et Bob puissent générer ensemble des bits aléatoires communs. Ni Alice ni Bob ne peuvent tricher sur la distribution. Ce schéma sert à pour l'équité des opérations aléatoires publiques.

- *Bit Commitment (BC)* : c'est le schéma de mise en gage d'un secret (un bit). Alice a un bit de secret et elle doit mettre en gage ce bit à Bob. Le schéma assure que plus tard, si Alice doit révéler le secret à Bob, Alice ne peut pas tromper Bob sur la valeur du secret.

Ce schéma aide à construire une application plus avancée : les preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs - ZKP). Informellement, c'est une application dans laquelle un "fournisseur de preuve" prouve à un vérificateur la validité d'une proposition sans révéler aucune autre connaissance que cette validité.

En effet, avec OT et CF, nous pouvons construire le calcul sécurisé pour toutes les fonctionnalités probabilistes, mais seulement dans le modèle "semi-honest". Pour garantir le comportements des utilisateurs, nous devrions utiliser les schémas de ZKP pour vérifier la correction des messages communiqués par chacun sans violer les secrets.

Un panorama du cadre de travail générique pour le calcul sécurisé est illustré par la figure 1. Les flèches montrent les relations de "réduction de sécurité" entre les primitivess. Nous constatons que le calcul sécurisé générique est construit sur les primitifs de OT, BC, CF, ZKP, dans lesquels OT est la brique centrale qui peut implémenter toutes les autres.

Dans le cadre de la Cryptographie Moderne, ces primitives sont réalisables en se basant sur la Théorie de la Complexité de Calcul.

0.2.2 La Sécurité Inconditionnelle vs. Hypothèses sur le Bruit

La sécurité inconditionnelle est associée à la Théorie d'Information, fondée par Shannon. Selon cette théorie, une information inconnue est assignée à une source d'information, décrite par une variable probabiliste $X = \{x_i; p(x_i)\}, i = 1..N$. L'incertitude d'une telle information est mesuré par l'entropie :

$$H_X = -\sum_{1}^{N} p(x_i) \log p(x_i)$$

Ainsi, la quantité d'information révélée de X par une autre information Y est mesurée par :

$$H_{X/Y} = -\sum p(x_i, y_j) \log p(x_i/y_j)$$

On dit que le système est sécurisé pour l'information X si pour toute information Y donnée à l'adversaire, la quantité d'information révélée de X est négligeable, i.e :

$$I(X;Y) = H(X) - H(X/Y) \approx 0$$

Malheureusement, les primitives "asymétriques" due calcul sécurisé ne peuvent pas être implémentées de façon inconditionnellement sécurisée par des communications triviales. En effet, les informations échangées au cours de l'exécution des protocoles sont "symétriques", et ne peuvent pas créer une telle asymétrie d'information.

La première version de Oblivious Transfer est un canal d'effacement asymétrique, proposé par Rabin :

L'émetteur envoie un message (bit) au récepteur qui a seulement une chance 1/2 de recevoir le message tandis que l'émetteur ne sait pas si le message est reçu ou non.

Ainsi, ultimement, il faut se baser sur une asymétrie d'information, utilisant les hypothèses, d'une autre manière, sur l'asymétrie causée par l'imperfection des matériaux, par exemple par les canaux de communication bruités.

Cette direction de recherche, initiée par Crépeau - Morozov et al., a exploré une riche collection de modèles de communication bruités. Les résultats majeurs ont montré que presque tous les modèles de communication usuels peuvent implémenter OT et ainsi BC, CF, cf. Figure 2.

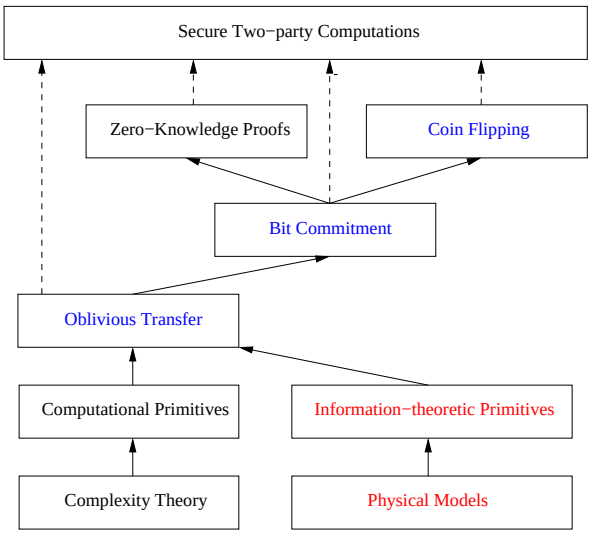

Figure 2: Une fondation inconditionnelle

Le cadre de travail central est de construire OT à partir des habituels canaux bruités, les canaux discrets sans mémoire (DMC - discrete memoryless channel). Les travaux de Crépeau, Morozov et al. ont montré une construction efficace de OT sur DMC. Leur idée est de concevoir un canal d'effacement. La suite est inspirée de la construction de Crépeau pour OT à partir du canal d'effacement de Rabin.

En bref, un DMC est décrit par deux ensembles discrets de signaux d'entrée $\mathcal{X}$, et de sortie $\mathcal{Y}$ avec une distribution de probabilité fixe pour chaque paire entrée/sortie $(x, y) \in \mathcal{X} \times \mathcal{Y}$.

A partir de ce canal, on construit un protocole un-canal à deux niveaux d'effacement. Seule la réception avec l'effacement faible est considérée comme bonne.

- Avec le choix d'une paire de signaux d'entrée x_1, x_2, on code le message binaire par un mot - $x_1.x_2$ pour 0 et $x_2.x_1$ pour 1.
- Par ce codage, il existe une (ou plusieurs) paires de signaux de sortie y_1, y_2 avec lesquels on a une probabilité optimale d'estimer le message envoyé en recevant $y_1.y_2$ ou $y_2.y_1$.
- Avec ce codage $\{x_1.x_2, x_2.x_1\} \times \{y_1.y_2, y_2.y_1\}$, on a un canal binaire d'effacement où toute réception d'autres mots que $\{y_1.y_2, y_2.y_1\}$ est considéré comme un effacement.

Le schéma de OT pour Alice qui envoie deux bits b_0, b_1 et Bob qui choisit le message b_c par le choix c est comme suit :

1. Alice génère N bits aléatoires r_i, $i = 1, ..., 2N$, et les envoie à Bob via le canal d'effacement. Bob reçoit r'_i ou un état d'effacement.

2. Bob crée deux sous-séquences I_0, I_1, $|I_0| = |I_1| = n$, telles que I_0 contient des positions i avec r'_i reçus. Bob renvoie (I_c, I_{1-c}) à Alice.

3. Alice envoie des codes correcteurs $(s_0 = syn(r_{I_c}), s_1 = syn(r_{I_{1-c}}))$ à Bob.

4. Alice envoie un masque m aléatoire de n bits à Bob.

5. Alice envoie $(\hat{b}_0 = k_0 \oplus b_0, \hat{b}_1 = k_1 \oplus b_1)$ à Bob, où $k_0 = (r_{I_c} \odot m)$, $k_1 = (r_{I_{1-c}} \odot m)$.

6. Bob corrige r'_{I_0} avec s_c, calcule la clé $k_c = (r'_{I_0} \odot m)$, et déchiffre $b_c = k_c \oplus \hat{b}_c$.

Le choix de n/N dépend de la probabilité de la réception d'un effacement faible. Supposons que cette probabilité est p_g, alors il faut $n/N < p_g$ pour que Bob puisse construire I_0 et $2n/N > p_g$ pour que Bob ne puisse pas corriger les erreurs dans les deux clés. Il faut aussi que N soit suffisamment grand pour avoir une grande sécurité de la clé r_{I_1}.

En utilisant le canal d'effacement sur une séquence de bits de clé, le récepteur reçoit une sous-sequence de bits avec "effacement faible" où il peut corriger les erreurs par des codes correcteurs. Par ailleurs, les codes correcteurs ne doivent pas permettre de corriger les erreurs davantage que cela.

L'émetteur envoie maintenant ses deux messages chiffrés par deux clés, deux sous-séquences indiquées par le récepteur. Utilisant une sous-séquence sans erreurs et une autre forcément avec erreurs comme, le récepteur ne peut choisir de recevoir qu'un seul message. Comme l'émetteur ne connaît pas l'état d'effacement des bits de la séquence de clef, il ne peut pas distinguer les sous-séquences indiquées.

0.2.3 Étrangeté Quantique

La science de l'information et de l'informatique est, en dernier ressort, reliée aux états des systèmes physiques et leurs évolutions. Les informations et les données sont matérialisées par les états des supports physiques et traitées (calculées) par les évolutions de ces supports.

Dans le monde classique, on est familier de la possibilité de déterminer l'état des systèmes physiques. Tout ce qui inconnu est assigné à une loi de probabilité sur l'ensemble des états possibles. Tout ce qui est connu évolue par des progrès déterministe. Le monde informatique est finalement discrétisé, avec une minuscule perte de précision, et modélisé par les machines de Turing, éventuellement probabilistes.

Or, à l'échelle des systèmes atomiques, le comportements des états physiques ne sont plus "classiques". Au 20ème siècle, une branche majeure de la physique s'est formée: la Physique Quantique. Ses lois qui aident à décrire et prédire les états "quantiques" ne sont plus classique ni intuitives.

L'implication de celles ci dans le domaine d'informatique est non moins contre-intuitive avec des "étrangetés quantiques".

Considérons un système physique "à deux états", $|0\rangle$ et $|1\rangle$, pour le support d'un "bit" logique d'information. On devrait pouvoir mesurer l'état du système et déterminer le bit d'information. En outre, nous voudrions utiliser un système microscopique pour le support dit "quantique".

Maintenant, conformément à la Physique Quantique, il se peut que l'état du système soit $\alpha|0\rangle + \beta|1\rangle$ qui donne $|\alpha|^2$ de chance pour un résultat de mesure 0 et $|\beta|^2$ pour 1 si nous mesurons le "qubit". Est-ce que c'est un continuum d'états possibles et que l'on n'a pas construit une machine pour mesurer pour tous ces états possibles ? La réponse est Oui et Non.

Oui, il y a un continuum d'états possibles. Mais Non, il n'existe pas une telle machine, théoriquement. En fait, ce continuum d'états serait un espace de Hilbert et chaque machine de mesure serait une projection sur une base orthogonale, peut-être d'un espace étendu par le couplage avec d'autres systèmes. Le Principe d'Incertitude de la Physique Quantique refuse une telle certitude sur la précision pratique des machines. Il affirme que théoriquement, les états non-orthogonaux ne sont pas distinguables.

On résume ici les postulats de la Physique Quantique

1. Chaque système quantique est décrit par un espace Hilbert comme son espace d'état dont chaque vecteur unitaire est un état possible. Considérons un espace de dimension fini N avec une base orthonormale $\{|i\rangle\}_N$, alors pour toute collection de coefficients $\{\alpha_i\}_N, \sum_{i=1}^N |\alpha_i|^2 = 1$, le vecteur

$$|\psi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$$

est décrit un état "pur" possible.

On adopte aussi une formulation matricielle $|\psi\rangle |\psi\rangle *$ pour cet état, normalement dénotée comme $|\psi\rangle \langle\psi|$ - la "matrice de densité".

2. Une machine de mesure "simple" est décrite comme une collection des projections sur les sous-espaces orthogonaux de l'espace d'états. On dit que c'est une mesure projective :

$$P = \{P_i\}, \sum_i P_i = I, P_i P_j = \delta_{ij}.$$

Si nous mesurons le système, qui est en état $|\psi\rangle$, par cette machine, nous obtenons un des projetés de $|\psi\rangle$ avec la probabilité déterminée par l'angle entre $|\psi\rangle$ et le sous-espace.

Par exemple, si nous avons une mesure projective complète (ou non dégénérée)

$$P = \{|i\rangle \langle i|\}_N,$$

alors nous allons obtenir une sortie $|i\rangle$ avec probabilité $|\langle\psi|i\rangle|^2 = |\alpha|^2$.

3. Un système peut être aussi dans un état probabiliste, dit mixte. Par exemple si nous avons mesuré le système et oublié le résultat : nous disons que le système est en un des états $|i\rangle$ avec la probabilité $|\alpha_i|^2$. Ce n'est plus l'état "pur" $|\psi\rangle = \sum_i \alpha_i |i\rangle$.

   En général, c'est un ensemble statistique $\{p_j; |\psi_j\rangle\}_M$. Convenablement, nous pouvons utiliser la formulation matricielle "de densité". On dénote maintenant l'état du système comme.

$$\rho = \sum_j p_j \rho_j = \sum_j p_j |\psi_j\rangle \langle\psi_j| .$$

   On réalise que $\sum_i |\alpha_i|^2 |i\rangle \langle i|$ et $|\psi\rangle \langle\psi|$ sont essentiellement différent.

   La mesure d'un état mixte par une machine donne toujours un des projetés sur les sous-espaces, avec une probabilité qui est enfin la somme statistique sur les états pures.

4. L'évolution de l'état d'un système est normalement décrit par une transformation unitaire sur l'espace des états. Supposons qu'un système est créé à l'état $|\psi\rangle$ et une transformation U est appliquée à ce système, nous obtenons le système en état final $U|\psi\rangle$. Dans le langage matriciel, l'état initial est $\rho = |\psi\rangle \langle\psi|$ et l'état final est

$$U\rho U^\dagger.$$

   Plus compliqué, la transformation de l'état d'un système peut être causée par une transformation unitaire, mais qui s'applique sur l'espace étendu par le couplage avec d'autres systèmes.

Par ces postulats sur la mesure et l'évolution des états quantiques, il y a deux propriétés remarquables des informations quantiques, reliés au Principe d'Incertitude :

1. Non-distinguabilité : supposons un système préparé en un état parmi un ensemble des états non-orthogonaux, il n'existe pas une mesure pour déterminer son état. On ne peut qu'estimer en se basant sur les résultats probabilistes.

2. Non-clonabilité : supposons un système préparé en un état parmi un ensemble des états non-orthogonaux, on ne peut pas copier son état.

Ce n'est pas tout. Considérons maintenant deux systèmes physiques A et B. Pour décrire l'état du système composite, on écrit l'état de A $|\psi\rangle_A$ à côté de l'état de B, $|\phi\rangle_B$, pour obtenir une concaténation de tenseur $|\psi\rangle_A \otimes |\psi\rangle_B$. Dans le monde quantique, ce n'est plus exact. Avec $|0\rangle_A \otimes |0\rangle_B$ et $|1\rangle_A \otimes |1\rangle_B$, un état possible est:

$$\alpha |0\rangle_A \otimes |0\rangle_B + \beta |1\rangle_A \otimes |1\rangle_B$$

que ne peut pas décrire $|\psi\rangle_A \otimes |\psi\rangle_B$. En plus, si nous séparons les deux systèmes A et B, et mesurons l'un des deux, par exemple A avec lequel si nous obtenons $|0\rangle$ (resp. $|1\rangle$) alors le système B sera définitivement en état $|0\rangle$ (resp. $|1\rangle$).

Une telle "intrication quantique" a surpris tout le monde des physiciens, surtout Einstein (EPR), et enfin protége de la violation de l'inégalité de Bell [EPR35, Bel64].

Conformément, la description de l'état de chaque sous-système d'un système composite est obtenue par l'opérateur de "trace out" sur les sous-sytèmes compléments.

$$\rho^A = tr_B(\rho^{AB}), \quad \rho^B = tr_A(\rho^{AB})$$

où $tr_X(|a\rangle_X |b\rangle_Y \langle c|_X \langle d|_Y) = |\langle a|c\rangle|(|b\rangle\langle d|_Y)$.

Tous ce formalisme des états quantiques a forcé à reconsidérer le monde informatique. Cela donne lieu à l'information quantique et le calcul quantique.

L'information classique, représentée par des signaux macroscopiques qui sont des états orthogonaux, est un cas propre de l'information quantique : un bit classique est représenté seulement par un des deux états orthogonaux d'une base dans un espace Hilbert à deux dimensions H_2, et un qubit est représenté par un état quelconque de l'espace d'états. Les bits classiques sont donc déterminable et copiable tandis que les qubits en général ne le sont pas.

L'introduction de l'information quantique à la construction des schémas cryptographiques est due à Wiesner. Basé sur le Principe d'Incertitude, Wiesner a proposé un schéma de codage conjugué comme canal de multiplexage [Wie83].

> Supposons qu'un émetteur envoie deux messages, chacun codé par un des états orthogonaux d'une base différente. Le récepteur doit mesurer les états pour recevoir les messages. Il doit choisir l'une des deux bases. Quand les bases sont "conjuguées", la mesure dans une base va détruire l'information dans l'autre base et ne fournira aucune information.

En fait, le canal de multilexage de Wiesner a été la base de l'idée d'un schéma de OT, mais incomplet. En plus, les applications de OT pour le monde cryptographique ont été découvertes beaucoup plus tard. Les contributions pour la construction d'un protocole de OT est de compléter le schéma de Wiesner. L'idée est d'utiliser le codage conjugué comme un canal d'effacement.

1. Supposons deux bases conjuguées pour les qubits : celle rectangulaire de $\{ket0, |1\rangle\}$ et celle diagonale de $\{|+\rangle, |-\rangle\}$ où $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.
2. Alice a un bit b à envoyer. Elle choisit aléatoirement une des deux bases, rectangulaire ou diagonale, et envoie le qubit qui encode le bit dans cette base.
3. Bob choisit une base aléatoire et mesure le qubit.
4. Alice annonce la base. Si Bob a utilisé la même, il sait qu'il obtient le bon résultat, et sinon, l'information a été effacée. Alice n'est pas au courant du choix de Bob.

Évidemment, si Bob a le moyen de stocker les qubits pendant longtemps, il peut tricher en attendant l'annonce de Alice sur la base. Un résultat dérivé est que si nous avons accès à un protocole de BC, on peut sécuriser le protocole quantique de OT, en forçant Bob à faire la mise en gage tous les résultats des mesures, et en permettant à Alice d'en vérifier certains avant d'annoncer les bases sur le reste.

Alternativement, les cryptographes cherchent à construire des protocoles de BC quantiques, qui utilisent les mêmes propriétés du canal quantique [BB84, BCJL93]. Malheureusement les implémentations allaient toujours à l'échec.

Un résultat No-go a été trouvé indépendamment par Mayers [May97] et Lo & Chau [LC97], prouvant que les protocoles quantiques pour BC ne sont pas réalisables. Plus tard, ce résultat No-go est élargi pour les protocoles de calcul sécurisé générique à deux parties, y compris OT [Lo97], même étant donné l'accès à un protocole de CF [Ken99].

L'idée est que, si Alice et Bob sont autorisés à utiliser des machines quantiques sans limite, Alice et Bob peuvent garder les calculs classiques et les mesures au niveau quantique en réalisant les simulations par la purification. Dans ce cas, tout protocole générique peut être considéré comme l'évolution déterministe d'un état pur d'un système à deux parties, les machines de Alice et Bob. Cet état pur ne permet pas le calcul sécurisé.

Par exemple, pour le protocole de BC, l'état du protocole juste avant l'ouverture du secret b est $|\Psi(b)\rangle_{AB}$. Il faut que les descriptions locales de Bob pour les mises en gage des deux valeurs de Alice soient identiques (ou quasi-identiques)

$$tr_A(|\Psi(0)\rangle\langle\Psi_0|^{AB}) \approx tr_A(|\Psi(1)\rangle\langle\Psi_1|^{AB}).$$

Alors, Alice a une transformation locale U_A pour changer des computations

$$U_A|\Psi(0)\rangle_{AB} \approx |\Psi(1)\rangle_{AB}$$

Alice peut donc utiliser U_A ou $U_A^\dagger$ juste avant la phase d'ouverture pour tricher.

0.3 Motivation et Contributions

0.3.1 Une Généralisation des Canaux d'effacement

Constatons que les canaux bruités sont une ressource pour l'implémentation des primitives inconditionnelles. Nous cherchons a rendre les constructions efficaces en économisant l'utilisation de cette ressource.

Le point est que la construction de Crépeau - Morozov exploite la différence de probabilités d'erreurs - celle optimale pour les paires de sortie $\{y_1.y_2, y_2.y_1\}$ et celle supérieure pour toute paire autre que $\{y_1.y_2, y_2.y_1\}$. Il y a des cas où cette différence est trop petite, qui induit un choix très restreint sur les codes correcteurs. En plus, une telle différence trop petite force Alice à envoyer plusieurs bits pour avoir une sécurité nette sur r_{I_1}.

On peut paramétrer le schéma pour avoir un meilleur choix. Pour cela, nous donnons la définition d'un canal d'effacement plus générique. On dénote ce canal comme canal binaire à multiple taux d'erreurs - BSMERC (Binary Symmetric Multi-Error-Rate Channel) :

1. Le canal est défini par un ensemble de taux d'erreur $\mathcal{E} = \{\varphi_i\}, 0 \leq \varphi_i \leq 1$ et une distribution de probabilités $\{p(\varphi_i)\}$.

2. Chaque fois l'émetteur envoie un bit r, le bit reçu r' sera erroné avec probabilité $\{p(\varphi_i)\}$ d'un taux d'erreur $\varphi_i \in \mathcal{E}$, i.e. $p(r \neq r') = \varphi$.

3. Le récepteur est informé de l'état d'effacement, i.e le taux d'erreur, alors que l'émetteur n'est pas.

On peut considérer ce canal comme une collection des BSC avec les taux d'erreur $\varphi_i \in \mathcal{E}$. Chaque fois l'émetteur envoie un bit, le canal choisit un des BSC avec φ_i selon la probabilité $p(\varphi_i)$ et transmet ce bit via le BSC. Le récepteur connait le BSC utilisé.

Par le codage d'entrée de Morozov et al. avec un canal DMC, nous avons exactement un canal BSMERC en considérant toutes les probabilités d'erreurs pour tous les paires de signaux de sortie possibles.

L'implémentation de OT sur ce canal s'inspire directement du schéma de Crépeau - Morozov, paramétré par un choix de seuil sur les taux d'erreurs. Par ce seuil, φ', tous les bits reçus sont considérés comme bons avec un taux d'erreur inférieur, et mauvais sinon. Les codes correcteurs d'erreurs sont ainsi choisis basé sur ce seuil. Par ce paramétrage, nous sommes plus libre pour exploiter une grande différence entre les probabilités d'erreurs "bonnes" et les "mauvaises" et rendre le schéma plus efficace [Dan07] :

1. Alice génère N bits aléatoires r_i, $i = 1, ..., 2N$, et envoie à Bob via le canal d'effacement. Bob reçoit r'_i avec un taux d'erreur Δ_i.
2. Bob crée deux sous-séquences I_0, I_1, $|I_0| = |I_1| = n$, telles que I_0 contient des positions i avec $\Delta < \varphi'$. Bob renvoie (I_c, I_{1-c}) à Alice.
3. Alice envoie des codes correcteurs $(s_0 = syn(r_{I_c}), s_1 = syn(r_{I_{1-c}}))$ à Bob.
4. Alice envoie un masque m aléatoire de n bits à Bob.
5. Alice envoie $(\hat{b}_0 = k_0 \oplus b_0, \hat{b}_1 = k_1 \oplus b_1)$ à Bob, où $k_0 = (r_{I_c} \odot m)$, $k_1 = (r_{I_{1-c}} \odot m)$.
6. Bob corrige r'_{I_0} avec s_c, calcule la clé $k_c = (r'_{I_0} \odot m)$, et déchiffre $b_c = k_c \oplus \hat{b}_c$.

0.3.2 Les Canaux Quantiques

Alternativement, nous proposons à considérer les constructions basées sur un schéma de codage non-orthogonal avec deux états non-orthogonaux, $|\psi_0\rangle, |\psi_1\rangle$:

$$|\langle\psi_0|\psi_1\rangle| = 1 - \beta, 0 < \beta < 1$$

Par exemple, avec $\cos 2\alpha = 1 - \beta$

$$|\psi_0\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle, |\psi_0\rangle = \cos\alpha|0\rangle - \sin\alpha|1\rangle,$$

L'émetteur encode la valeur 0 ou 1 d'un bit par l'état correspondant $|\psi_0\rangle$ ou $|\psi_1\rangle$ et envoie le qubit. Un tel codage ne permet pas un décodage parfait qui distingue les deux états.

Avec ce codage, le récepteur peut construire de différentes machines de mesure pour estimer la valeur du bit encodé. Par exemple,

- S'il utilise la mesure projective de la base $\{|+\rangle, |-\rangle$, il gagne l'information mutuelle optimale sur le bit. Nous avons ainsi un canal binaire symétrique - BSC dont le taux d'erreur est $1/2 - \cos\alpha \sin\alpha$ [BMS96].

- Le récepteur peut aussi mesurer pour avoir une estimation conclusive sur le bit envoyé. Par exemple, avec mesure dans la base $\{|\psi_0\rangle, |\perp \psi_0\rangle\}$, si la sortie donne une sortie sur $|\perp \psi_0\rangle$ qui est orthogonal à $|\psi_0\rangle$ alors le récepteur sait que le bit est 1. Le récepteur peut utiliser une mesure de POV pour optimiser la probabilité d'avoir une estimation exacte [Iva87, Die88, Per88, JS95, Bus97] :

$$\left\{ \begin{array}{l} \hat{E}_0 = \frac{1}{2-\beta}(I - \rho_1), \\ \hat{E}_1 = \frac{1}{2-\beta}(I - \rho_0), \\ \hat{E}_2 = I - \hat{E}_0 - \hat{E}_1 \end{array} \right\},$$

  Le bit envoyé sera parfaitement décodé si la mesure donne les signaux 0 et 1, ou effacé si un signal 2. La probabilité du bon décodage est β.

  Nous avons ainsi un canal d'effacement.

- Plus intéressant, si l'on envoie une séquence de bits par ce codage et considère la parité de ces bits comme le message, Bob peut construire une mesure "cohérente" sur l'ensemble de qubits pour avoir une estimation optimale [BMS96]. Cette mesure donne en fait la simulation d'un canal à multiples effacements - BSMERC.

Nous pouvons utiliser un de ces canaux bruités, simulés par le codage non-orthogonal, pour l'implémentation d'un protocole de OT. Un schéma simple basé sur le canal d'effacement est comme suivant :

1. Alice génère N bits aléatoires et envoie ces bits à Bob, utilisant le codage non-orthogonal.
2. Pour chaque qubit i, Bob détecte $r'_i \in \{0, 1, 2\}$.
3. Bob construit deux sous-séquences $I_0, I_1 \subset \{1, ..., N\}$ telque $|I_0| = |I_1| = n$, et $\forall i \in I_0, r'_i \in \{0, 1\}$.
4. Bob envoie la paire (I_c, I_{1-c}) à Alice, conformément à son choix c.
5. Alice envoie $(\hat{b}_0 = b_0 \oplus k_0, \hat{b}_1 = b_1 \oplus k_1)$ à Bob avec $k_0 = \bigoplus_{i \in I_c} r_i$, $k_1 = \bigoplus_{i \in I_{1-c}} r_i$.
6. Bob déchiffre le message $b_c = \hat{b}_c \oplus \bigoplus_{i \in I_0} r'_i$.

Pourtant, l'utilisation du codage quantique rend le schéma de OT vulnérable. En effet, Alice peut violer le codage pour affecter les probabilités des canaux bruités et ainsi distinguer les sous-séquences indiquées par Bob. Et, dans l'autre sens, Bob peut utiliser toute mesure cohérente possible sur l'ensemble des qubits pour gagner de l'information sur les messages finaux.

Nous montrons les attaques possibles, au cas par cas :

- On peut sécuriser le protocole contre toutes les attaques possibles de Bob. En se basant sur le résultat de [BMS96] qui montre une mesure optimale de Bob, nous pouvons anéantir l'information finale de Bob sur les messages. Le protocole est ainsi sécurisé si Alice respecte le codage. Nous voulons forcer Alice à être honnête.

- Pour une première impression, nous donnons à Bob la possibilité de vérifier le codage sur certaines positions aléatoire. Supposons un protocol de CF pour donner des position à vérifier. Mais, une attaque est possible pour Alice, basée sur l'intrication. Alice peut utiliser une paire

$$\begin{aligned}|\phi\rangle &= \sqrt{1-\frac{\beta}{2}}\,|0\rangle_A\,|0\rangle_B + \sqrt{\frac{\beta}{2}}\,|1\rangle_A\,|1\rangle_B \\ &= \frac{1}{\sqrt{2}}(|+\rangle_A \otimes |\psi_0\rangle_B + |-\rangle_B \otimes |\psi_1\rangle_B)\end{aligned}$$

  et envoie le qubit B pour tous les bits de clef.

  En cas de vérification, Alice mesure le qubit A dans la base $\{|+\rangle, |-\rangle\}$ et annonce 0 pour $|+\rangle$ et 1 pour $|-\rangle$. Sinon, Alice mesure le qubit A dans la base $\{|0\rangle, |1\rangle\}$ pour gagner de l'information sur l'état d'effacement de Bob.

- Nous pouvons sécuriser le protocole seulement si nous avons accès à un protocole de BC : Alice doit faire la mise en gage des bits de clés et Bob peut vérifier sur un sous ensemble aléatoire (généré par le CF).

0.3.3 Les Théorèmes No-go Quantiques

La démonstration centrale des théorèmes est de réduire tout protocole générique à un protocole pur à deux parties. En fait, dans un protocole générique, il y a des opérations classiques :

1. les utilisateurs font des mesures, passent les calculs aux classiques, probabilistes;
2. les utilisateurs ont des variables privées, secrètes;
3. les utilisateurs communiquent via un canal classique qui dénie des états quantiques.

Dans la littérature, les articles originaux et les interprétations successives, ont fait attention plutôt aux deux premières catégories. En effet, les variables probabilistes classiques utilisées dans les protocoles sont purifiables par l'extension des systèmes quantiques privés. Mais, ce n'est pas le cas pour la communication via un canal classique.

Nous proposons à reconsidérer le modèle bipartite quantique général concernant le calcul et les communication classiques et quantiques.

On constate que dans un modèle général, un canal classique est forcément macroscopique et sa décohérence est si forte que l'information quantique n'y est pas acceptée. Ainsi, le modèle quantique pour les protocoles à deux parties devient *à trois parties*, consistant en trois composants physiques: la machine d'Alice, la machine de Bob, et l'environnement couplé avec le canal classique qui mesure les messages classiques communiqués, cf. Figure 3. L'exécution du protocole sera une évolution déterministe sur l'état global qui est un état pur connu, à trois parties.

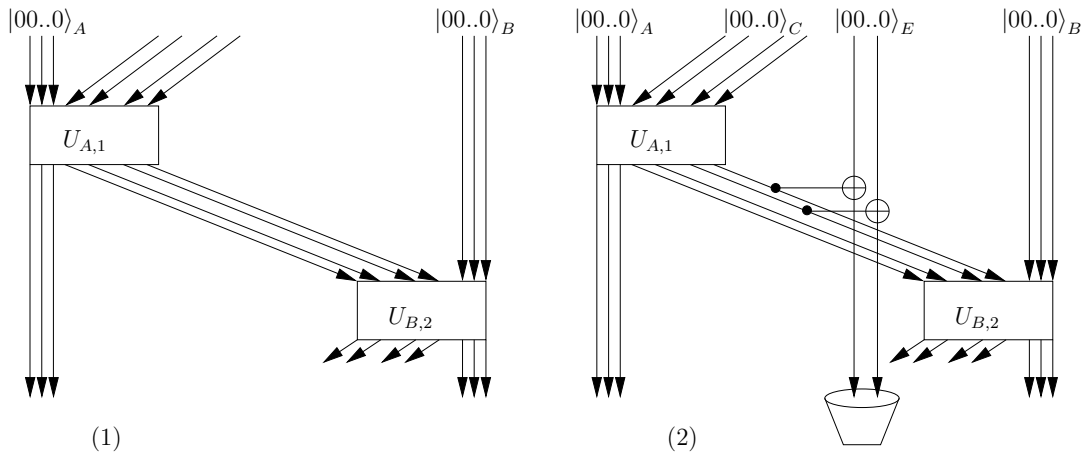

Figure 3:
(1) le modèle quantique dans la littérature et (2) le modèle générique

1. L'émetteur $S \in \{A, B\}$ doit mesurer dans un protocole dont l'état est $|\psi\rangle_{AB}$ avec une machine à n signaux. Cette mesure va sortir $i \in \{1, .., n\}$ avec la probabilité $p(i)$ et rendre le système en état $|\psi_i\rangle_{AB}$:

$$|\psi\rangle \to \sum_i \sqrt{p(i)}\, |\psi_i\rangle_{AB} |i\rangle_S |i\rangle_{E,S}$$

où $\mathcal{H}_{E,S}$ représente les systèmes macroscopiques et l'environnement dans la machine à mesure.

2. L'émetteur envoie le signal i au travers le canal classique. Le signal est copié, amplifié par les systèmes d'environnement E sur canal :

$$|i\rangle_S \to |i\rangle_S \otimes |i\rangle_E .$$

3. Le signal se propage jusqu'à la machine du récepteur $R = \{A, B\} \setminus \{S\}$, où un état $|i\rangle$ est créé pour cette machine :

$$|i\rangle_E \to |i\rangle_E \otimes |i\rangle_R .$$

Remarquons que les signaux classiques sont publics, copiés et amplifiés par les trois systèmes Alice, Bob, et Environnement. Chaque message possible i devrait être représenté par un état $|i\rangle_A i_B i_E$. Le système de E apparaît seulement pour ces messages publiques, dans la forme

$$|\Psi\rangle = \sum \sqrt{p_i}\, |i\rangle_E |i\rangle_A |i\rangle_B |\psi\rangle_{AB}$$

Un tel rôle de E n'aide pas à la construction des protocoles sécurisés. En fait, la description locale sur la machine de Bob donne la même information que la description locale sur l'ensemble formé de la machine de Bob et de l'environnement E, cf. Figure 4. Supposons

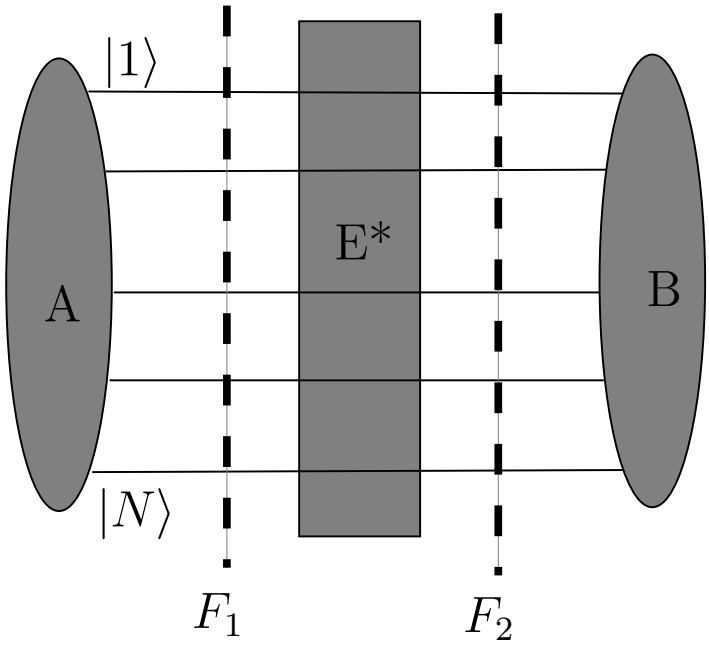

Figure 4: La communication des messages classiques

que le protocole de BC est sécurisé du coté de Bob, il est aussi sécurisé si Bob contrôle E, et Alice peut tricher comme dans le cas des protocoles purs à deux parties.

D'ailleurs, dans un protocole de BC, l'état global pour la mise engage d'un bit b est :x

$$|\Psi(b)\rangle_{ABE} = \sqrt{p_i(b)}\,|i\rangle_E\,|i\rangle_A\,|i\rangle_B\,|\psi(b)\rangle_{AB}$$

Et pour la sécurité du bit b :

$$tr_{AE}(|\Psi(0)\rangle\langle\Psi_0|^{ABE}) \approx tr_{AE}(|\Psi(1)\rangle\langle\Psi_1|^{ABE})$$
$$\Rightarrow tr_A(|\Psi(0)\rangle\langle\Psi_0|^{ABE}) \approx tr_A(|\Psi(1)\rangle\langle\Psi_1|^{ABE}).$$

Alors, Alice a une transformation locale U_A pour changer des computations :

$$U_A\,|\Psi(0)\rangle_{ABE} \approx |\Psi(1)\rangle_{ABE}$$

Ces théorèmes No-go ont dénié la construction des protocoles quantiques à deux parties. Pour le calcul inconditionnellement sécurisé à deux parties, il faut en fait retourner aux modèles qui utilisent une troisième partie honnête.

Inspiré du modèle à trois parties dans notre interprétation ci-dessus, nous pouvons aller plus loin pour appliquer ces théorèmes négatifs à certaines troisièmes parties non triviales.

Nous constatons que toute participation d'une troisième système qui apparaît sous la forme

$$|\Psi\rangle = \sum \sqrt{p_i}\,|i\rangle_E\,|i\rangle_A\,|i\rangle_B\,|\psi\rangle_{AB}$$

ne cache pas d'information. Et donc, le calcul sécurisé ne peut pas être obtenu par une telle intervention.

Ces troisièmes parties peuvent couvrir plusieurs entités intéressantes :

1. Un canal classique, comme nous l'avons montré dans l'interprétation.

2. Un protocole de CF. En effet, supposons qu'il y ait un "oracle" qui fournit à Alice et Bob des bits aléatoires publiques. Un tel bit classique devrait être sous la forme

$$|c\rangle = (|0\rangle_A |0\rangle_B |0\rangle_E + |1\rangle_A |1\rangle_B |1\rangle_E)/\sqrt{2}$$

   Quand ce bit est intégré au protocole, il ne change pas la forme pénalisée ci-dessus. Ce résultat étend un peu plus le résultat de Kent [Ken99] qui considère seulement chaque bit aléatoire comme un bit quantique, une paire EPR à deux parties Alice et Bob. En fait, notre système permet une "intrication" avec un environnement extérieur pour avoir un vrai bit classique.

3. Un circuit quantique qui implémente un calcul quelconque, qui n'a qu'à recevoir des données d'Alice et Bob et renvoyer toutes les sorties.

4. Un "oracle" à ressource limitée (en terme d'espace d'état) qui devrait jeter toutes les informations à l'environnement publique pour réinitialiser.

Cette extension entraîne un corollaire concernant les aspects thermodynamiques: l'implémentation de *bit commitment*, de *oblivious transfer*, et en général du calcul à deux parties inconditionnellement sécurisé, nécessite la suppression d'information ainsi que la dissipation de chaleur dans l'environnement extérieur [Lan61].

0.4 Conclusions

La recherche effectuée dans cette thèse traverse trois domaines :

1. Dans une première partie, nous nous intéressons aux cadres basés sur les modèles de bruits pour la construction des primitives inconditionnelles.

   Nous monrons que la construction de OT à partir des canaux DMC est loin d'être optimale. Nous proposons une paramétrisation qui peut impliquer une amélioration de ce schéma, via un modèle intermédiaire.

2. Dans la deuxième partie de cette thèse, nous proposons un cas d'étude à travers des implémentations par un codage quantique non-orthogonal. C'est un codage convenable à simuler les canaux bruités. Et nous montrons au cas par cas les attaques possibles quand on l'utilise pour une implémentation de OT. Nous montrons également comment le protocole de OT est sécurisé par l'accès à ce protocole, alors que c'est impossible avec un protocoles de CF.

   En fait, l'implémentation des primitives quantiques se heurte au résultat négatif des théorèmes No-go de Mayers et Lo & Chau.

3. Dans la troisième partie, nous révisons les théorèmes No-go de Mayers et Lo & Chau. Ces théorèmes No-go restent parmi les objets les plus intéressants du domaine de la Cryptographie Quantique.

   Longtemps après, il y a encore des chercheurs qui veulent invalider ces théorèmes, même si toute proposition les défiant se trouve tôt ou tard fausse. Cette controverse sur la validité de ces théorèmes est dû au manque d'une interprétation complète pour les purifications dans les protocoles génériques.

   Si dans la construction d'un protocole, on considère le canal quantique comme "bruité" par l'effet du principe d'incertitude, les théorèmes rejettent le protocole dans un enjeu plus large, couvrant les purifications des probabilités.

   Nous proposons dans cette thèse de reconsidérer ces théorèmes avec une réinterprétation plus appropriée des protocoles quantiques. Notre modèle réaffirme la validité des théorèmes. Et d'ailleurs, nous pouvons étendre ces résultats No-go à certains protocoles qui ont accès à des troisièmes parties non-triviales, comme un protocoles de CF.

Chapter 1

Introduction

Cryptography was created as a discipline of hiding information in communications. Classical Cryptography has been being concerned with the problem of securing two-party communications from the interception of malicious third-parties. For many years, this is all there had been to cryptography. However, cryptography had been considered rather as an art than a science until Shannon's works shown how to prove the security of ciphersystems, based on information theory [Sha49]. Shannon's security is defined as the uncertainty about the secret information, measured by the entropy characterizing the randomness of the information source. This leads to the notion of *information-theoretical security or unconditional security* as it does not depend on the computational power of the adversary.

An important mark for the beginning of Modern Cryptography was made by Diffie and Hellman with their proposal of a key exchange protocol. In their article, the authors introduced the ideas of public-key systems and of provable security based on computational complexity, named *computational security* [DH76]. The computational security is defined as it is *reducible* to a computational problem commonly adopted as *hard*: the adversary can break the cryptosystem only if he has a computer solving the underlying problem in a reasonable time.

This foundation of security is related to unproven assumptions of intractable problems on the underlying computing model, i.e. Turing machine. Thus, this foundation is not unconditional and bears potential threats: (i) the assumptions of intractable problems are not proven as one does not know whether efficient algorithms may exist for these problems; and furthermore, (ii) there may exist advanced computational models beyond Turing machines.

Nevertheless, with this new computational complexity foundation, Modern Cryptography has motivated a significant section of researchers in the field of computing science and become an important part of this widespreading domain. Besides providing communication security, such as guaranteeing integrity and authenticity, as the central goal, Modern Cryptography has expanded to encompass many others more sophisticated and fascinating applications of information privacy.

One of the major contributions of Modern Cryptography has been the implementation of advanced security of protocols between distrustful users. These protocols enable users to electronically solve many real world problems, play games, and accomplish very general

intriguing distributed tasks such as zero-knowledge proofs, voting protocols, and generally secure multi-party computations [Gol01, Gol04].

In this thesis, we will focus on quantum primitive protocols for secure two-party computations which is a subclass of general secure multi-party computations, concerning only two distrustful users. This is a new interdisciplinary field that bridges quantum physics, computer science, and cryptography.

1.1 Secure Two-party Computations

In a formal definition, a distributed n-party computation is concerned with an n-ary functionality F that maps n inputs $(x_1, ..., y_n)$ to n outputs $(y_1, ..., y_n)$ in a context where the inputs and outputs are distributed among n distrustful users in the distance. The security is for users' local inputs in the sense that what is learned by a user $i(1 \leq i \leq n)$ during the protocol can be learned by that user from his local input x_i and his final output y_i of the computation. This requirement is as though in an *ideal* setup where there exists an honest party T, trusted by all users, who gathers all x_i to locally compute $(y_1, ..., y_n) = F(x_1, ..., x_n)$ and sends back each y_i to each user i [Gol04].

Secure two-party computations are in a subclass of secure multi-party computations, concerning only two distrustful users, named Alice and Bob.

1.1.1 Founding on Oblivious Transfer

One common approach in engineering and hence in cryptography engineering is to separate applications from ultimate implementations by layering and introducing fundamental intermediate primitives which would be implemented with more freedom.

> The best that has been done so far is to prove theorems based on more general cryptographic assumptions, such as "trapdoor functions exist," rather than specific assumptions, such as "factoring is hard." [Kil88]

This bearing leads to the discovery of oblivious transfer which is the most important primitive for building general secure two-party computations. Oblivious transfer becomes then one of the central primitives and a foundation of Modern Cryptography.

The first idea of oblivious transfer was issued in the 1970s by Wiesner, with a setting of the quantum channel, named "quantum conjugate coding" or "multiplexing channel" [Wie83]. However, Wiesner did not go further for cryptographic applications of his scheme. Then, the first proposal of oblivious transfer, with its name, is to Rabin for implementing advanced cryptographic tasks [Rab81]. Rabin's version is *a transmission scheme where Alice sends a bit to Bob who has only a probability* $1/2$ *of receiving it, and Bob knows whether he has received the bit or nothing while Alice does not.* Later, Even et al. proposed a scheme similar to Wiesner's one, *permitting Alice to send two messages to Bob who can choose to read out only one message while Alice is unaware of Bob's choice,* for building more general secure computation tasks [EGL85]. This scheme is named "one-out-of-two oblivious transfer," and considered as the standard version of oblivious transfer. It was also shown that "one-out-of-two oblivious transfer" and Rabin's oblivious transfer are equivalent [Cré88].

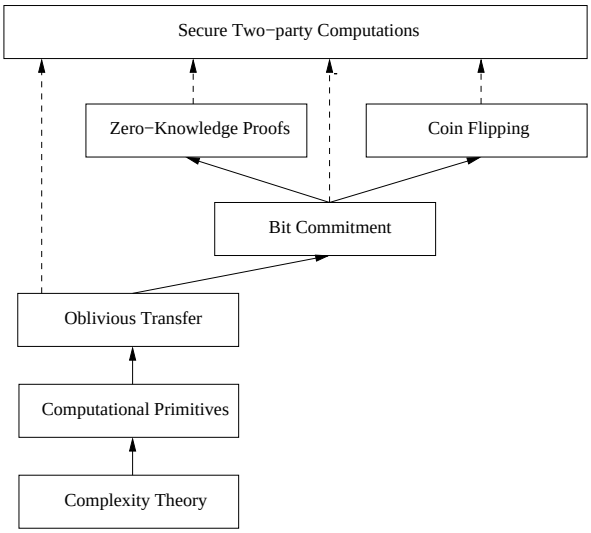

Figure 1.1: Founding secure two-party computations on oblivious transfer

It was latter shown that oblivious transfer is sufficiently used as a building block to construct secure two-party protocols for general functionalities [Yao86, Kil88, Gol01, Gol04]. As a sketch: oblivious transfer can be used for building bit commitment, coin flipping, zero-knowledge proofs; and the implementation of any secure two-party computation can be made upon these four primitives, cf. Figure 1.1 [Gol04]. Simply speaking:

- *Bit commitment* is a protocol for committing the evidence of a secrete value: Alice has to commit the value of a secret bit to Bob such that Bob cannot learn this value, but later, when Alice is supposed to reveal the secrete, she cannot change her mind.
- *Coin flipping* is a protocol for two users in the distance generating a random bit such as no one can control the probability distribution of the outcome.
- *Zero-knowledge proofs* are protocols for a prover convincing a verifier about the validity of an assertion while not revealing any knowledge beyond the validity of the assertion.

1.1.2 Removing the Intractability Assumptions

Recall that Modern Cryptography is built on the foundation of computational complexity theory where the security is based on intractability assumptions. Oblivious transfer was also supposed to be built with conditional security [Kil88, Gol04], and becomes the cut point on the links between two-party protocols and the computational foundation of Modern Cryptography, cf. Figure 1.1. However, these assumptions were not proven, and the threats to this foundation had been realized very early by cryptographers [Kil88], before an explicit example was made for famous RSA public-key system [Sho94].

An emerging approach for removing the intractability assumptions is to seek for information-theoretical implementations of oblivious transfer. Unfortunately, we cannot

break down the symmetry in trivial noiseless communication for making such asymmetrical transmission schemes [Kil88, Mor05]. Nevertheless, we can build *unconditionally secure* oblivious transfer with information-theoretical assumptions about transmission media. The researches are motivated in two directions:

1. One goes back to Rabin's oblivious transfer which is defined as an information-erasing channel: Alice sends a bit to Bob who receives the bit with probability 1/2 otherwise an erasure symbol [Rab81]. With this communication point of view, one extends the family of oblivious transfers with variants of erasure channels by weakening the condition on parameters such that the standard OT is still reducible to these cousins [Cré88, CK88, Dan06].

2. One looks for implementations of these weakened erasure channels from real-life communication models [CK88, BBCS92, Cré97, CMW04].

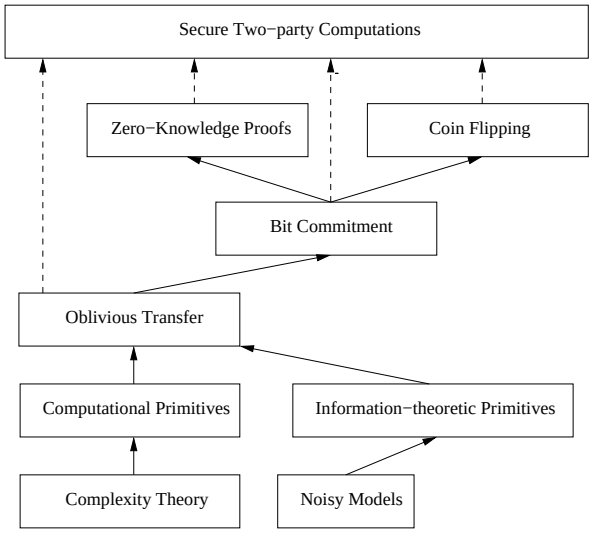

Figure 1.2: Seeking for information-theoretical realization of the assumptions

The approach had much interest in noisy models of communication channels for implementing the desired erasure channels. A major result states that oblivious transfer can be made from nontrivial noisy channels: if Alice and Bob are connected by a fair nontrivial noisy channel with known parameters then they can implement a secure oblivious transfer protocol, except with arbitrarily small failure probability, cf. Figure 1.2 [CMW04, Mor05]. It's also shown that we can build oblivious transfer with unfair noisy channels for bounded control of Alice and Bob on the parameters of the channels [Mor05].

We say that oblivious transfer and then secure two-party computations can be built from almost any noisy channel with unconditional security, *except with assumptions about noisy model of the channel itself.*

1.2 Quantum Ere and No-go Results

Besides, the discovery of application of quantum mechanical concepts to information processing has led to a new framework for both computation and communication [NC04].

The computational processes have been created as a mathematical abstract invention. For long time, though there has been rigorous researches on computational models for describing what can be computed, the computational models remain abstract such as Turing machines, logical circuits, programming languages, etc. Nevertheless, all of the real processes have to obey ultimate physical rules of Nature. Such a first statement was made by Landauer in his principle "the erasure of a bit of information would lead to the dissipation of an amount of $kT \ln 2$ of heat," solving Maxwell's thermodynamical demon puzzle [Lan61].

For a resume, classical information processing is concerned with applying transitions on discrete input information which are normally encoded by sequences of binary symbols $\{0, 1\}$ under Boolean Algebra. For the implementation, these two symbols are represented by the *distinguishable* states $\{|0\rangle, |1\rangle\}$ of any two-state physical system. The development of electronic devices with transistor technology has made computers more and more powerful everyday. We are making denser and denser accurate devices with fewer cubic nanometers per unit. However, the physical implementation of this abstract computing model realizes the relation with physical laws as soon as actual computers are made with atomic scale devices where quantum mechanical laws are involved. In the atomic scale, the physical systems act quite differently, for instance a two-state system can be in a superposition state, i.e. it can be in any state $a|0\rangle + b|1\rangle$ where a, b are complex numbers and $|a|^2 + |b|^2 = 1$. Moreover, the transitions between quantum states are governed by the laws of quantum theory with new features apart the classical ones [Gri04, Per02].

Most of all, this new ere has made significant impacts to the field of Cryptology (Cryptography and Cryptanalysis). These impacts are twofolds. In one direction, a new computing model with robust algorithms [Sho94, Gro96] requires serious reconsideration of the computational security based on classical computing models [PQC06]. In the other one, the uncertainty principle and the non-cloneability of quantum mechanical information give new unconditionally secure cryptographic tools such as random number generator [JAW+00], key exchange schemes [BB84, Eke91, Ben92].

Motivated by this promoting framework, many researches are directed to the construction of unconditionally secure primitives for secure computations without any assumption except the postulates of ultimate laws of quantum theory.

The first proposal is for a coin flipping protocol which leads nearly to a bit commitment protocol [BB84]. However, this scheme is found to be flawed by an attack which exploits the special property of quantum entanglement. Later, despite many attempts to implement quantum secure two-party computations' primitives [BCJL93], one could finally find some flaws behind [May96].

Furthermore, a more general attack was claimed, exploiting the entanglement in the two-party models, to flaw all possible quantum bit commitment protocols [May97, LC97]. In fact, in the proofs of Mayers and Lo-Chau, the impossibility of quantum bit commitment is simply derived from a property of the pure bipartite quantum states which leads to the fact that if a bit commitment protocol is secure against Bob before the opening, then Alice can

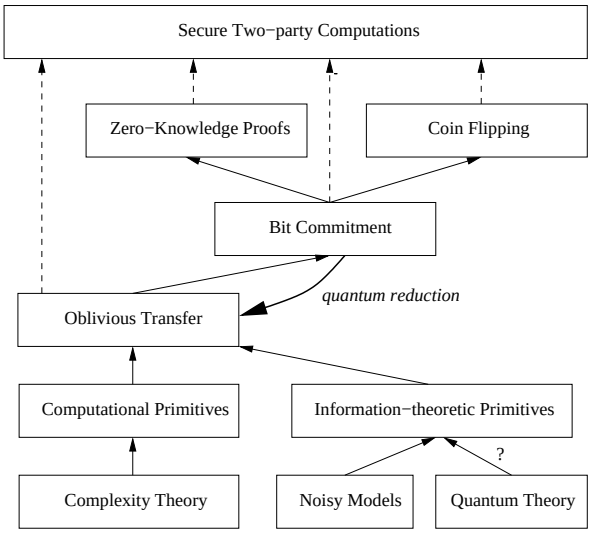

Figure 1.3: Seeking for quantum mechanics based realization of the assumptions

use a local transformation to change her secret.

A similar proof for the impossibility of quantum oblivious transfer protocols was later described in [Lo97]. Because of the similarities between the no-go theorems for quantum bit commitment and quantum oblivious transfer protocols, one used to talk only about the theorem of quantum bit commitment.

However, though the theorem is claimed to be valid for all general protocols using hybrid quantum and classical communication and computation [May97, LC97], the interpretation for the generality remains unclear and causes researchers not to cease to either challenge it [Yue00, Yue04, Che03], or confirm it [Bub01b, Che05, Che06], or reestablish it [dKSW06].

The obsession to this claim of generalization is that it is not clear to see how the proofs cover all possible protocols which can consist of

1. classical computations with secret random variables,

2. communications via a classical channel that does not permit a pure two-party model.

One could say that the theorem on the *impossibility* of unconditionally secure quantum bit commitment [LC97, May97], and the theorem on the *possibility* of unconditionally secure quantum key distribution [LC99, SP00], are among the most interesting subjects in the field of quantum cryptography. Moreover, these impossibility and possibility could lead to philosophical thoughts about quantum theory [Bub01b, CBH03, BF05].

A related problem is to consider the relation between cryptographic primitives in the quantum model of two-party protocols. While it was classically shown that bit commitment implements coin flipping and is implemented by oblivious transfer [Kil88], oblivious transfer can be built from bit commitment by transmitting quantum information [Cré94, Yao95].

Nevertheless, coin flipping, which is also banned from being implemented in the scope of quantum mechanics by other no-go results [LC98, Kit02], was shown to be strictly weaker than bit commitment in the two-party quantum model [Ken99].

1.3 Contributions and Outline

This thesis is concerned with and contributes to the theory of unconditionally secure two-party primitives, with either positive or negative results, particularly in the framework of quantum mechanical model for two-party protocols.

In Chapter 4, we provide in detail our reviews on related works, mainly concerning the constructions of oblivious transfer based on noisy channels [CMW04, Mor05]; the constructions of quantum variants based on Wiesner's quantum conjugate coding; and Mayers', Lo's and Chau's (MLC) no-go theorems on quantum primitives.

In Chapter 5, we expose a development [Dan07] contributing to the framework for the construction of oblivious transfer based on noisy models. We propose to consider more closely the model of a *binary symmetric multi-error-rate channel* which is implemented from discrete memoryless channels by the same construction of Crépeau *et al.* [CMW04]. With this channel, we can realize a general binary symmetric erasure channel by providing an error-rate barrier separating *good* from *bad* error rates. We present also an implementation of secure oblivious transfer from these extensions. Moreover, with such consideration of multi-error-rate channels, we have freedom to separate two sets of *good* and *bad* for an improvement of efficiency in building oblivious transfer, based on the probability distribution of the error rates. We expect also that the introduction of the model of multi-error-rate channel can help to solve the open problem on building oblivious transfer from noisy channels with continuous alphabets [Mor05]. However, a quantitative analysis is left to further consideration.

In Chapter 6, we present a framework of building oblivious transfer variants based on a quantum coding scheme using two nonorthogonal quantum pure states. We show that this framework is equivalent to the existing one based on quantum conjugate coding [BBCS92, Cré94, Yao95]. We highlight also the necessary of considering quantum coherent attacks in protocol reduction schemes using classical combination of subroutines. In many cases, we should be careful with traditional technique of classical privacy amplification and consider general attacks by quantum machines.

Finally, in Chapter 7, we present our reconsideration of general models for two-party protocols. We show that in reality, a general two-party protocol is concerned with a macroscopic channel and should not be interpreted as a quantum two-party system consisting only of two users' machines. We present then a faithful interpretation for the generality of Mayer's and Lo's & Chau's no-go theorems in this general model which is a quantum three-party quantum system, extended to include an environment system coupled with the classical channel. With this interpretation, we show that the theorems can be extended to cover some particular oracle based models. These particular quantum oracles do not change the features of the three-party model which is penalized by the attacks of the theorems. We remark that these oracles are indeed in a class of oracles which do not make erasure of information. This leads to a discussion on the thermodynamical feature of two-party primitives, based on Landauer's

principle [Lan61].

For a preliminary on the backgrounds of these works, the readers can refer to Chapter 2 for basics of computation theory, information theory and cryptography, and Chapter 3 for basics of quantum information processing.

Chapter 2

Probability, Computation, and Cryptography

Cryptography was an ancient art of hiding information during communications. Till nowadays, it has been much developed and concerned to cover a larger domain of applications in which the primordial goal of cryptography is to construct cryptosystems that will be robust against malicious acting to make these schemes fail their prescribed functionality. In this cooperative context, the cryptosystems are required to be designed in accordance with Kerckhoffs' principles [Ker83]:

> "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

Forever, protecting the privacy of secret information remains its main object. The question is "how much an untrustful adversary can infer about the secret of the other(s)?" In a more concrete argument, "how secure is the secret against the adversary provided gained supplementary information?" With this argument, one bases the privacy on two requirements:

1. The secret is perfectly secure, i.e. the knowledge about the secret is not affected by the available information. In terms of information theory, the secret must be statistically independent from the supplementary information. This point of view is known as information based security.

2. The secret is secure if it is difficult to be computed from the supplementary information, provided that computational power of the adversary is well defined. This point of view is known as computational-based security, developed by Modern Cryptography in connection with Computational Complexity Theory.

2.1 Probability Theory and Information-Theoretical based Security

2.1.1 Probability Theory

Probability theory is a domain providing mathematical language for *random phenomena* that lie beyond the limit of knowledge. A random phenomenon is associated to a *randomness* that selects the outcome from a set of possible values with assigned *probabilities*, representing the frequency of each possible value when the phenomenon is subject to a large number of *trials*.

For the notation, a random variable X over a domain $\mathcal{X}$ takes any value $x_i \in \mathcal{X}$ with probability $Pr(X = x_i)$ (or $P(X = x_i)$). We denote by P_X the probability distribution and $Pr(X = x_i)$ can be replaced with $P_X(x_i)$. By the normalization, $\sum_{x_i \in \mathcal{X}} P_X(x_i) = 1$ for discrete $\mathcal{X}$ or $\int_{x_i \in \mathcal{X}} P_X(x_i) = 1$ for continuous $\mathcal{X}$.

The relation between two random variables is described by their dependency. Suppose that when variable X has taken value $x_i \in \mathcal{X}$, a related variable Y will have a conditional probability distribution $P_{Y/X=x_i}$ where Y takes value y_j in its domain $\mathcal{Y}$ with probability $P_{Y/X=x_i}(y_j)$. In many cases it can be denoted as $P(Y = y_j/X = x_i)$ or $P(y_j/x_i)$. Y is independent from X if and only if P_Y and $P_{Y/X=x_i}$ is identical for all $x_i \in \mathcal{X}$.

In the field of computing and information theories, we are concerned with binary variables and Bernoulli probability distribution:

$$P_X(1) = p, \quad P_X(0) = 1 - p.$$

The probabilities manifest themselves when the number of trials is sufficiently large, following the Laws of Large Numbers. An useful law of large numbers for binary distribution is:

Theorem 2.1 (Rompel's Law of Large Numbers)**.** *Let $X_1, ..., X_n$ be Poisson trials, i.e. independent trials with $1 \leq i \leq n, P(X_i = 1) = p_i$ and $P(X_i = 0) = 1 - p_i$. Then, for $X = \sum_{i=1}^{n} X_i$, $\mu = E(X) = \sum_{i=1}^{n} p_i$, and any $\mu/n > \delta > 0$:*

$$P\left(\frac{|X - \mu|}{n} > \delta\right) \leq 2e^{-n\delta^2/2}$$

In case of Bernoulli trials, i.e., when $p_1 = p_2 = ... = p_n$, this reduces to the well-known Bernstein's law of large numbers:

Theorem 2.2 (Bernstein's Law of Large Numbers)**.** *Let $X_1, X_2, ..., X_n$ be independent random variables following a Bernoulli distribution with p as the probability parameter. Then for any $\delta > 0$*

$$P\left(\left|\frac{\sum_{i=1}^{n} X_i}{n} - p\right| \geq \delta\right) \leq 2e^{-n\delta^2/2}$$

2.1.2 Information Theory

In the 40s, Shannon proposed a foundation for information theory in which an information source is a statistical model for a physical entity that produces outputs called messages in a

random manner with some a priory statistical parameters [Sha48, CT91]. We are normally concerned with discrete sources whose messages take value in a set $\{x_1, .., x_n\}$ with probabilities $\{p_X(x_1), .., p_X(x_n)\}$. So, a message from this statistical source is characterized by a random variable X that takes value x_i with probability $p_X(x_i)$.

We are usually working with discrete and memoryless channels, i.e. the transmission of one message over the channel is statistically independent from the previous ones. Based on this probabilist model, the system is described by a discrete input symbols alphabet $\mathcal{X} = \{x_1, .., x_n\}$, an output one $\mathcal{Y} = \{y_1, .., y_m\}$ and a conditional probability distribution $P_{Y/X}$ where $P_{Y/X=x_i}(y_j)$ specifies the probability of receiving output y_j when input x_i has been sent. When the channel is noiseless, the probability distribution is trivial, i.e. $P_{Y/X=x_i}(y_i) = 1$ with $\mathcal{X} \equiv \mathcal{Y}$. We work frequently with binary symmetric channel (BSC) where $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ and the error probability is symmetric over $\mathcal{X}$: $p_e = P_{Y/X=0}(1) = P_{Y/X=1}(0)$.

Shannon introduced also the first idea of mathematically measuring the privacy of a secret [Sha48]. The main idea is to estimate the lack of *information* about a secret (message or key) from the encrypted message, named ciphertext. This is then rigorously treated by the theory of information, based on probability theory and statistics.

If a message, that must be assigned to some *a priori* known statistical source, is unknown to a person, this person has no more knowledge about the message than the *a priori* statistical description of its source: a message X can be instant x_i with a priori probability $P_X(x_i)$. One measure of the knowledge can be expressed as the entropy of the source, quantifying uncertainty about, or the privacy of, the message:

$$H(X) = -\sum_{i=1}^{n} P_X(x_i) \log P_X(x_i). \tag{2.1}$$

$H(X) = 0$ when one of $P_X(x_i) = 1$, i.e. the person is a priori certain about the occurrence x_i of X. $H(X)$ is maximal when all the p_i are equal, i.e. $H(X) = \log n$, and we say the message is perfectly secret. For binary distribution $\{p, 1-p\}$, the binary entropy is denoted as

$$h(p) = -p \log p - (1-p) \log(1-p) = h(1-p). \tag{2.2}$$

Here, the probability distribution is merely subjective: if a message randomly chosen by a person A is kept secret from another person B then the probability distribution assigned to the message by A is trivial while the one by B is a flat distribution.

If another evidence y related to the message X is given to the considered person, this changes the *subjective* probability distribution assigned to X by the person, known as conditional probability distribution: X takes value x_i with probability $P_{X/y}(x_i)$. The uncertainty about X is now

$$H(X/y) = -\sum_{i=1}^{n} P_{X/y}(x_i) \log P_{X/y}(x_i).$$

If the evidence is also given as a random variable Y that takes value $y_j \in \{y_1, ..., y_m\}$ with probability $p_Y(y_j)$, then the uncertainty about X of the person is averaged:

$$H(X/Y) = -\sum_{j=1}^{m} P_Y(y_j) H(X/y_j) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P_{X,Y}(x_i, y_j) \log P_{X/Y=y_j}(x_i) \tag{2.3}$$

This quantity is used for the remaining uncertainty, named equivocation by Shannon, about X knowing Y. It's convenient that knowing Y always reduces the uncertainty about X:

$$H(X/Y) \leq H(X),$$

and $I(X;Y) = H(X) - H(X/Y)$ is the mutual information between X and Y that quantifies the average amount of information about X revealed by Y.

Then, the privacy of the secret message X of a cryptosystem, that sends some message Y to an adversary, against that adversary is characterized by the amount of information about X revealed by Y, i.e. $I(X;Y)$. The system is perfectly secure only if $I(X;Y) = 0$ or $H(X/Y) = H(X)$, i.e. X, Y are pairwise independent. Because by definition, this security is associated to the *randomness* and independent of adversaries' computational power, it is named *unconditional security*.

The measure of entropy was then developed by Renyi with the definition of Renyi entropy of order a, where $a \geq 0$.

$$R_a(X) = \frac{1}{1-a} \log \left(\sum_{i=1}^{n} (P_X(x_i))^a \right).$$

When a approaches 1, Renyi entropy converges to Shannon entropy:

$$R_1(X) = H(X).$$

Specially, Renyi entropy of order 2 is usually used by for privacy amplification based on universal$_2$ hashing [CW77, BBCM95]:

$$R_2(X) = -\log \left(\sum_{i=1}^{n} (P_X(x_i))^2 \right).$$

2.1.3 One-Time-Pad

By this measure, a simple cipher named Vernam's cipher has been proven to be perfectly secure. Suppose we have a secret one-bit message described by random binary variable X: $P_X(1) = p = 1 - P_X(0)$. We choose then a secret one-bit key K with $P_K(0) = P_K(1) = 1/2$, and exclusive-or X and K to produce ciphertext $Y = X \oplus K$:

$$P_Y(1) = P_X(0)p_K(1) + P_X(1)P_K(0) = 1/2 = 1 - P_Y(0).$$

The conditional probabilities are

$$\begin{aligned}
P_{Y/X=b}(0) &= P_K(b) = 1/2 = 1 - P_{Y/X=b}(1), \\
P_{Y/K=b}(0) &= P_X(b) = 1 - P_{Y/K=b}(1), \\
P_{X/Y=0}(b) &= P_X(b) = P_{X/Y=1}(b), \\
P_{K/Y=0}(b) &= P_X(b) = P_{K/Y=1}(b)
\end{aligned}$$

for $b \in \{0,1\}$. Thus, the conditional uncertainties of the message and the key, given the ciphertext, are

$$H(X/Y) = h(p) = H(X), \quad H(K/Y) = h(p) \leq H(K).$$

Therefore, the message is perfectly secure while the key is not. The solution is that we use only one key once for one message, i.e. for a sequence of n bits, we use a key of n random bits. This perfect cipher is so known as one-time-pad, and it is shown that any perfect cipher must be as consuming in secret key as one-time-pad: $H(K) \geq H(X)$ [Sha49, Sti95]. Thus, unconditional security and Vernam's cipher is hard to be realized for communicating between two users because it requires a shared secret key of the same length as the message. Nevertheless, one-time-pad is efficiently used in the construction of *reductions* between cryptographic primitives [Gol01, Gol04].

2.1.4 Error Correction and Privacy Amplification

Recall that the gap between knowledges of legitimate user and untrustful user upon a secret is crucial for cryptosystems. In the computational point of view, this gap is expressed as the computational easiness-difficulty in one-way functions [Gol01]. In the information-theoretical point of view, this gap is measured by entropies: the situations are interesting when the legitimate user has less uncertainty about the secret than the malicious one. In such cases, there exist mathematical tools for enhancing in one way the knowledge of the legitimate user and in the other way the uncertainty of the malicious user: error correction and privacy amplification:

1. while legitimate user, who has some advantageous knowledge, can produce the correct secret by error correcting codes [MS77],

2. the remaining partial knowledge, after error correcting phase, of malicious user can be reduced to be negligible by privacy amplification [BBCM95].

These two techniques are used in exploiting noisy models for unconditionally secure applications such as key agreement [Wyn75, BBB$^+$92, Mau93], oblivious transfer [CMW04, Mor05]. We cite here two important related asymptotic results for error correction and privacy amplification [BBCM95, Mor05].

Theorem 2.3. *For any $\varphi > 0$ there exists $\rho > 1$ such that for all $\gamma > h(\varphi)$ and sufficiently large N there exists a linear code with the length N and a number of check bits at most γN, failing to correct φN uniformly distributed errors only with probability at most $\rho^{-(\gamma - h(\varphi))N}$.*

Simply speaking, Theorem 2.3 allows us to construct asymptotic codes to almost correct the errors caused by a BSC with error rate φ by sending sufficient check bits. This proportion of check bits must be greater than the amount of lost information $h(\varphi)$.

Theorem 2.4. *Let V be a uniformly distributed n-bit string and let W be generated by independently sending each bit of V over a φ-BSC. Let, furthermore, $syn : \{0,1\}^n \to \{0,1\}^r$*

be a linear function and G be a random variable corresponding to the uniformly random choice of a function from a universal class of hash functions[2] $\{0,1\}^n \to \{0,1\}^l$. *Then,*

$$I(G(W); (G, V = v, syn(W))) \leq 2^{-(R_2(W|V=v)-l-r)} / \ln 2$$

for all sufficiently large n. $R_2(W|V = v) > (h(\varphi) - \gamma)n$ for any fixed $\gamma > 0$ and sufficiently large n except probability exponentially small in n.

The idea of Theorem 2.4 is that if W represents a secret of which the adversary gets some partial information $V = v$ via a φ-BSC and some codes via the function $syn(W)$ then we can expel adversary's information on the sufficiently shortened secret $G(W)$.

2.2 Computation Theory and Computational Complexity based Security

The theory of computation is concerned with the automation of computing by algorithmic processes of describing and transforming information. The fundamental question is "what can be (efficiently) automated?"

In 1936, Turing proposed the Turing machine (TM) as a model of computation. It is an abstract machine for deterministically manipulating symbols, equipped with a state that is in any of a finite set of states, an infinite tape of cells that hold symbols from a finite alphabets, and tape-head that scans the tape. In each step, following a finite set of rules called *program*, the machine reads the symbol in the positioned cell, changes the state and moves the tape-head to left or right. The machine has a special state for which the machine halts, known as halting state. For some input string, which is the initial content of the tape, the machine can terminate with halting state after a finite number of steps or run forever. If the machine halts, the content of the tape is the output computed by the machine.

In terms of languages, the set of input strings on which a Turing machine halts is named "language recognizable by" that machine.

Although its simplicity, one believes the assumption that this machine is the model for any possible *classical* computation, known as Turing thesis. The modern theory of computation is indeed the theory of what can be computed by Turing machine [HMU01]. Moreover, the major object of computing theory is concerned with the efficiency of Turing machines for computational problems. Beside many *easy* problems which can be efficiently computed by TM (in polynomial time), there are many *difficult* problems believed to not be efficiently computed (in polynomial time), named as intractable problems. Two important classes of easy and *believably* difficult problems are:

- $\mathcal{P}$: class of languages that can be recognizable by a polynomial-time Turing machine.
- $\mathcal{NP}$: class of languages L that is associated with a witness language Y and a verifying language $R_L \subset L \times Y$:
  1. $\forall x \in L, \exists y \in Y$ such as $(x, y) \in R_L$,
  2. if $x \notin L$ then $\forall y \in Y, (x, y) \notin R_L$,

3. R_L is recognizable in polynomial-time in measure of length of x.

$\mathcal{NP}$ has an important subclass known as $\mathcal{NP}$-complete with the property that any $\mathcal{NP}$ problem p_1 can be reducible to a $\mathcal{NP}$-complete problem p_2 in polynomial-time. Then a famous theorem of Cook proved that the *boolean satisfiability problem* is $\mathcal{NP}$-complete ([HMU01], Theorem 10.9).

Then, modern cryptography is related to the theory of computational complexity where the security of secrets is based on assumptions of difficult problems. For instance, the security of the famous RSA public-key system is based on the difficulty of factoring large integers.

Evidently, the security based on hard problems is conditional and dependently related to the unproven assumptions of their difficulty, e.g. $\mathcal{P} \neq \mathcal{NP}$ or factoring large integers is hard, as well as the computing model, i.e. Turing machine is the model for any possible computation. This conditional security can be threatened by potential advances in algorithmic or computing models. In fact, new concepts of quantum computing permit to factor integers in polynomial time [Sho94], breaking RSA system, or speed up exhaustive searches of witness for $\mathcal{NP}$ problems [Gro96].

Nevertheless, founded on computational complexity, modern cryptography has made drastic advances where the embraced gap between easy and difficult problems leads to asymmetrical cryptosystems of fruitful applications [Gol04].

2.3 Secure Two-party Computations' Primitives

2.3.1 The Essential Primitives

Oblivious Transfer

The first proposal of oblivious transfer to be used in construction of cryptographic applications was made by Rabin [Rab81], in which the sender sends a bit and the receiver has only probability 1/2 for receiving it while the sender does not know what has happened. Later, another version was proposed by Even et al. [EGL85], known as chosen one-out-of-two oblivious transfer, and preferred as a standard oblivious transfer. In this standard version, the sender sends two bits and the receiver secretly selects to receive one and only one of sender's bits. Moreover, the two versions are equivalent [Cré88].

In terms of two-party functionality, oblivious transfer is defined as an one-sided mapping $\{0,1\}^2 \times \{0,1\} \mapsto \emptyset \times \{0,1\}$ where the sender introduces two bits (b_0, b_1), the receiver introduces a choice bit c, and at the end the receiver receives $b_0 * (1-c) + b_1 * c$ while the sender learned nothing.

Bit Commitment

Simply speaking, bit commitment is a protocol where Alice commits the evidence of the value of a secret bit to Bob who cannot discover Alice's secret, but then if Alice is supposed to reveal the secret, she must prove its value and Bob can detect if Alice cheats.

In terms of information-theoretical security, the protocol must hold

- The concealment: Bob gains no information about Alice's bit with the committed information.
- The binding: At the opening phase, if Alice changes the secret value, Bob can successfully detect it.

It has been stated that a bit commitment protocol can be built, provided an oblivious transfer protocol [Cré89]:

Protocol 2.1. $OT \rightarrow BC(b)$

- *Commitment phase:*
  1. *Alice prepares a sequence of n random bits* $x_1, ..., x_n$ *and generates another sequence* $y_1, ..., y_n$ *such that* $\forall i (1 \leq i \leq n), x_i \oplus y_i = b$. *Bob prepares a sequence of random bits* $c_1, ..., c_n$.
  2. *For* $1 \leq i$, *Alice and Bob execute* $OT(x_i, y_i)(c_i)$, *and Bob receives then a sequence* $z_1, ..., z_n$.
- *Opening phase:*
  1. *Alice reveals b and sends all of* $(x_1, ..., x_n)$, $(y_1, ..., y_n)$ *to Bob.*
  2. *Bob accepts if and only if* $\forall 1 \leq i \leq n, z_i = x_i(1 - c_i) + y_i c_i$ *and* $x_i \oplus y_i = b$.

We see that the protocol is concealing because for each pair x_i, y_i Bob can receive only one bit, and cannot determine the x-or of them. Besides, the binding can be assumed except with probability exponentially small in n.

Coin Flipping

Informally, coin flipping is a protocol for Alice and Bob agree on a truly random bit.

If they are present at the same location, it is trivial for one user to toss a fair coin with the observation of the other. However, if the two are far apart the one from the other then they cannot realize the above scheme as the tossing user can lie about the outcome. In that case, it is not trival to generate a random bit of which the probability distribution is independent from the intentions of Alice and Bob with noiseless communication channels.

However, if we have a bit commitment protocol, we can easily implement a protocol for Alice and Bob flipping a random bit:

Protocol 2.2. $BC \rightarrow CF$

1. *Alice prepares a random bit a and sends the commitment* $c(a)$ *to Bob.*
2. *Bob prepares a random bit b and sends it to Alice.*
3. *Alice opens the commitment a with* $c(a)$ *and Bob verifies. Then each user computes* $r = a \oplus b$.

Moreover, much of interests in secure computation are concerned with the situation in which one user has to generate random bits to be kept secret but the other one would rather has commitment of the values [Gol04]. Simply, we can slightly modify the above scheme to have such an augmented coin flipping protocol:

Protocol 2.3. *$BC \rightarrow$ augmented-CF*

1. *Alice prepares a random bit a and sends the commitment $c(a)$ to Bob.*
2. *Bob prepares a random bit b and sends to Alice who computes $r = a \oplus b$.*

Zero-Knowledge Proofs

The zero-knowledge proofs were introduced into the field of cryptography with much interest. The first service is for proving assertions, commonly as "instance x belongs to language L" in terms of computing theory, without disclosing any additional knowledge than the validity of the assertions. The second is that, its formulation gave the idea of a *simulator machine* which is widely used as standard formalism for proving protocol security.

An interactive proof system consists of two interactive machines, P for prover and V for verifier, where the prover want to convince the verifier the validity of an assertion commonly expressed as "a string x belongs to a language L." The two machines have a common input x and finally V produces 1 if $x \in L$ and 0 otherwise. The introduction of probabilist computation would weaken this condition with some negligible probability of error.

An interactive proof system (P, V) for language L is zero-knowledge if for every verifier $V*$, there is a simulator M_{V*} such that for $x \in L$, the distribution of output by M_{V*} on input x is indistinguishable from the distribution of output by $V*$ interacting with P on input x.

An important result states that [Gol01]:

Theorem 2.5. *Given bit commitment protocol, zero-knowledge proofs exist for all languages in $\mathcal{NP}$*

The idea for this statement is a construction for the $3 - SAT$ language, known as $\mathcal{NP}$-complete, and then any other $\mathcal{NP}$ language can be reduced to that, cf. Section 2.2.

2.3.2 Reductions

Secure Two-Party Computations

We present here a sketch of the decomposition of secure two-party computations.

Any functionality can be decomposed into a logical circuits consisting of AND and XOR gates, provided inputs and random tapes which is distributed to Alice and Bob. One build then an oblivious evaluation protocol that replaces each gate by an augmented gate that works on the *shares* instead of the plaintext-data: given the plaintext a then the shares are a_A hold by Alice and a_B by Bob such that $a_A \oplus a_B = a$, where $\oplus$ denotes the exclusive-or (x-or) operator. In fact, we can implement evaluation gates with help of a 1-to-4 oblivious transfer protocol, cf. Protocols 2.4, 2.5.

Protocol 2.4. *Gate XOR:* $(a_A, b_A), (a_B, b_B) \rightarrow (a \oplus b)_A, (a \oplus b)_B$.

- *Alice computes* $(a \oplus b)_A = a_A \oplus b_A$
- *Bob computes* $(a \oplus b)_B = a_B \oplus b_B$

then $(a \oplus b)_A \oplus (a \oplus b)_B = a_A \oplus b_A \oplus a_B \oplus b_B = (a \oplus b)$.

Protocol 2.5. *Gate AND:* $(a_A, b_A), (a_B, b_B) \rightarrow (a.b)_A, (a.b)_B$

- *Alice prepares a random bit* r*, and a table of* 4 *members*

$$i, j \in \{0, 1\}, X_{ij} = (a_A \oplus i).(b_A \oplus j) \oplus r$$

- *Alice sends Bob the table via 1-to-4 OT where Bob can choose to receive only one of the members. Bob enters* $a_B b_B$ *as his choice to receive* $X_{a_B b_B}$.
- *Alice holds* r *as* $(a.b)_A$ *and Bob hold* $X_{a_B b_B}$ *as* $(a.b)_B$.

then $(a.b)_A \oplus (a.b)_B = r \oplus ((a_A \oplus a_B).(b_A \oplus b_B) \oplus r) = a.b$.

Suppose that Alice and Bob want to compute a function $f(x, y)$, and Alice holds input x, Bob holds input y. Initially, Alice generates a random key x_A as a *share*; computes and sends the other *share* $x_B = x \oplus x_A$ to Bob. Bob does the same for the *shares* y_A, y_B of y. Then, with the evaluation protocol based on augmented gates for function f, Alice and Bob compute with the *shares* and then get the *shares* of the final results of f. They are required only a round for combining the final *shares* to obtain the decrypted results.

However, the above construction is secure only if Alice and Bob are semi-honest i.e. each user respects the protocol but wants to learn the other's secret. In reality, the users can be malicious with unlimited behaviours, for instance they generate unfair random tapes, substitute the intermediate results. Thus, it's more difficult to construct a secure protocol in such a malicious model. It was showed that with help of commitment, coin flipping and zero-knowledge protocols, we can force malicious user to act as semi-honest [Gol04]. The general compilation for the malicious model can be sketch as follows:

1. Each user makes the commitment of the inputs to the other.
2. Each user makes random tapes with augmented coin flipping protocol giving the commitment to the other.
3. The users realize the oblivious evaluation protocol, but at each communication step, the sender has to prove the correctness of the output message by zero-knowledge proofs. It's because the correctness of the next message, which is deterministically produced from committed data and the previous incoming messages, is a $\mathcal{NP}$ statement.

Besides, given oblivious transfer, we can build bit commitment, and then coin flipping and zero-knowledge proofs for $\mathcal{NP}$ languages. In summary, the reduction schemes show that the secure computation of any two-party functionality can be built from oblivious transfer solely. In other words, secure two-party computations can be founded on oblivious transfer, cf. Figure 1.1.

Proof of Security

In many circumstances, we expect building new, more interesting protocols upon existing protocols served as subroutines. This technique is named *reduction* or *protocol reduction*.

In a formal way, the subroutines are treated as ideal oracles that implement the specified functionalities of the subroutines, and the composed protocol invokes these oracles when necessary. Ideally, we would expect that the composite protocol is itself implemented by an ideal oracle for the specified functionality.

In the field of cryptography, we have to consider the security for the new protocol by guaranteeing that what a malicious party can do with the composed protocol is the same as, or indistinguishable from, what this party can do when invoking the ideal oracle for the protocol. The standard approach for arguing the security of the composed protocols which are built upon the subroutines leads to the zero-knowledge criteria. It's required that for the malicious user, there exists a simulator which produces by itself indistinguishable output from what produced by the machine interacting with the other honest users [Cré90, Gol01, Gol04].

In this thesis, we are only concerned with two-party protocols where the security is considered when a party tries to cheat the other being honest. We will also simplify our proofs of security without appealing to this beautiful but complicated framework using simulator machines. In each concrete protocol, we will explicitly consider the information revealed to the malicious adversary.

Chapter 3

Quantum Information Processing

The computing or information processing machinery has obtained the ever greater success in 20^{th} century, issuing the electronic implementation of Von Neumann model which realizes the Universal Turing Machine, an abstract computing machine stated to be able to compute what is naturally regarded as computable.

In a way, any abstract computing machine musts be abstracted from mechanically effective steps which can be automated, that is what "machine" means. The most familiar abstraction is to Turing with Turing's thesis for his computing machine:

Thesis 3.1 (Turing's thesis)**.** *LCMs [logical computing machines: Turing's expression for Turing machines] can do anything that could be described as "rule of thumb" or "purely mechanical". (Turing 1948: 7.)*

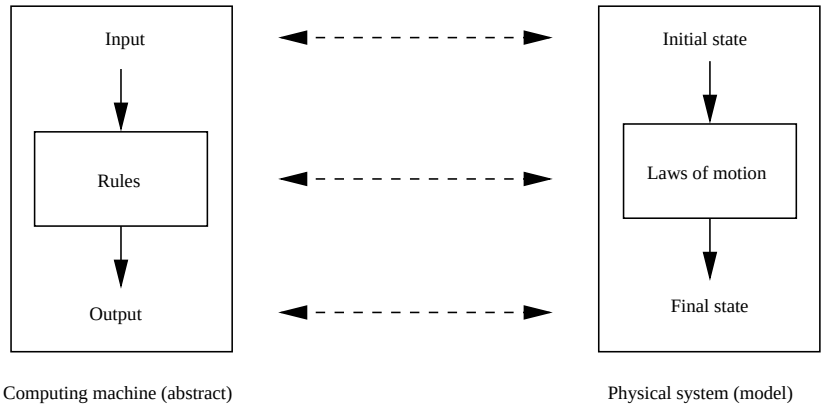

Figure 3.1: Connection between Information Processing and Physical Motion

Inversely, any abstract computing machine may be conceivable within a physical framework. Any real information processing system relies for its implementation upon systems whose behavior is completely described by the laws of physics. The connection between

what can be done mechanically and an abstract computing model can be sketched as in Figure 3.1 [Deu].

In this dissertation, we will be concerned with quantum information, in which the fundamental models for information processing are based upon the laws of quantum mechanics. In the view of Figure 3.1, information are introduced as quantum states of physical systems, observed by observable values from quantum measurement, and processing rules are realized by quantum mechanical laws of motion.

This chapter introduces some fundamental features of quantum information, emphasizing quantum mechanical concepts of physical state, laws of motion and measurement.

3.1 Quantum State Space, Evolution and Measurement

We have first to be familiar to a mathematical language provided by quantum theory for describing physical systems of *quantum scale* of which the behavior is probabilistic but manifests interference of waves. Remark that the notion "physical system" is rather an abstraction, may not be a real entity. For instance, in a desired experience, the physical system is the polarization of a photon, not the photon itself; or in another experience, where we consider "position-momentum" of a photon, the physical system is now reported to "position-momentum." One may admit an inverse definition as

> "A quantum system is whatever admits a closed dynamical description within quantum theory" [Per02].

Then, with the physical system in test,

> "a state is characterized by the probabilities of the various outcomes of every conceivable test" [Per02].

For unifying the interference of probabilities of outcomes in quantum tests, quantum theory has formulated each quantum state as a wave function which changes over time according to Schrodinger's equation, and belongs to a state space which is a Hilbert space. Although one may be aware of the fact that

> "quantum phenomena do not occur in a Hilbert space, they occur in a laboratory" [Per02],

it suffices for getting the hang of quantum language within its mathematical formulation in Hilbert spaces, provided quantum postulates. A Hilbert space is defined as

1. It is a vector space $\mathcal{H}$ over complex number field $\mathbb{C}$.
2. It is assigned an inner product function $(.,.)$ from $\mathcal{H} \times \mathcal{H}$ to $\mathbb{C}$ that maps an ordered pair of vectors (φ, ψ) to a complex number with properties:
   (a) $(\psi, \psi) \geq 0$ and the equality happens iff. $\psi = 0$.
   (b) $(\varphi, a.\psi_1 + b.\psi_2) = a(\varphi, \psi_1) + b(\varphi, \psi_2)$ for $a, b \in \mathbb{C}$.

(c) $(\varphi, \psi) = (\psi, \varphi)*$ where the asterisk $(*)$ symbolizes for the complex conjugate.

In the area of quantum theory, one is familiar to Dirac's ket notations:

- $|\psi\rangle$ stands for vector ψ.
- $\langle\varphi|\,\psi\rangle$ stands for inner product (φ, ψ).
- $|\psi\rangle\langle\varphi|$ stands for projection operator which maps vector $|v\rangle$ to $\langle\varphi|\,v\rangle\,.\,|\psi\rangle$.

For describing the state of a quantum physical system, we adopt the first postulate of quantum theory language:

Postulate 3.1 (Quantum pure state)**.** *Any isolated physical system is associated a state space which is a Hilbert space. The system is completely described by a unit vector in the associated state space, i.e. its norm* $\|\psi\| = \sqrt{\langle\psi|\,\psi\rangle} = 1$*. This state vector encodes the probabilities for the outcomes of all possible measurements applied to the system.*

Then, the state of a quantum system evolves in time following quantum theory of motion:

Postulate 3.2 (Unitary evolution)**.** *The evolution of a closed system is described by a unitary operator on the state space of the system. That is, given the initial state* $|\psi\rangle$ *and the evolution operator* U*,* $UU^\dagger = U^\dagger U = I$*, the final state is*

$$\left|\psi'\right\rangle = U\,|\psi\rangle\,.$$

For human knowledge about a quantum system, one needs to measure the system with *observables* which interact with the quantum system, amplify the magnitudes and show the results as macroscopic signals. After the measurement, the state of the quantum system is modified according to the result. So, the ultimate measurement is an observable which is a collection of projections corresponding to possible real outcomes, known as projective measurement:

Postulate 3.3 (Projective measurement)**.** *Every physical observable is represented by a Hermitian operator on the state space of the system being observed, i.e. the observable operator can be diagonalizable with real eigenvalues. It has a spectral decomposition*

$$M = \sum_i a_i P_i,$$

where the eigenvalues $a_i \in \mathbb{R}$ *represent the outcome signals, and* P_i *is the projector onto the eigen-space of* M *with eigenvalue* a_i*. We see that* $P_i = \sum_j |v_{ij}\rangle\langle v_{ij}|$ *for* $\{|v_{ij}\rangle\}_j$ *being the collection of corresponding eigenvectors of* a_i*.*

When measuring the state $|\psi\rangle$*, the probability of getting outcome* a_i *is*

$$p(a_i) = \langle\psi|\,P_i\,|\psi\rangle$$

and given that outcome a_i *occurs, the state of the measured system is projected by* P_i*, or collapsed to:*

$$\frac{P_i\,|\psi\rangle}{\sqrt{p(a_i)}}.$$

Normally, rather than giving an observable in Hermitian formalism, one specifies a collection of complete orthogonal projection operators $\{P_i\}$, $\sum_i P_i = I, P_i P_j = \delta_{ij} P_i$ for an implicit observable $M = \sum_i iP_i$. Particularly, one frequently uses the term "measure in the basis $\{|v_i\rangle\}$", where $\{|v_i\rangle\}$ forms an orthonormal basis of the state space, for the observable given by the projection operator list $\{P_i = |v_i\rangle \langle v_i|\}$. Then, any state vector is an unit (or normalized) vector $|v\rangle = \sum_i c_i |v_i\rangle, c_i \in \mathbb{C}$. The measurement of the system in state $|v\rangle$ "in the basis" will give outcome i with probability $p_i = |c_i|^2$, $\sum_i |c_i|^2 = 1$, and if the outcome a_i occurs then the system is in state $|v_i\rangle$. c_i are known as probability amplitudes, but furthermore they inherit the property of complex numbers and manifest the interference within the linear algebra over Hilbert spaces.

3.2 Statistical Ensembles, Density Matrix

In quantum world, probabilities are not always manifested as complex amplitudes. Sometime, we are given a system in a *mixed state* which is described by a statistical ensemble, i.e. the system is in one of states $\{|\psi_i\rangle\}_i$ with respective probability p_i. This ensemble is normally denoted as $\{p_i, |\psi_i\rangle\}$. We are then provided the density operator language as a convenient mathematical description for this kind of quantum state. Within this language, the above statistical ensemble is represented by a matrix

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \quad \text{with} \quad \forall i, p_i \geq 0 \text{ and } \sum_i p_i = 1.$$

When the system is measured with an observable $M = \sum_j a_j P_j$, according to Postulate 3.3, each member state $|\psi_i\rangle$ (with probability p_i) gives outcome a_j with probability

$$p(a_j/i) = \langle\psi_i| P_j |\psi_i\rangle$$

and the corresponding output state is

$$|\psi_{ij}\rangle = \frac{P_j |\psi_i\rangle}{\sqrt{p(a_j/i)}}.$$

Thus globally, outcome a_j occurs with probability

$$p(a_j) = \sum_i p_i p(a_j/i) = \sum_i p_i \langle\psi_i| P_j |\psi_i\rangle = \sum_i p_i tr(P_j |\psi_i\rangle \langle\psi_i|) = tr(P_j \rho)$$

where $tr(.)$ is the trace operator, and the corresponding output state of the system is an ensemble $\{p(i/a_j), |\psi_{ij}\rangle\}_i$ with $p(i/a_j) = \frac{p_i p(a_j/i)}{p(a_j)}$. Then, by the density operator language, the matrix representation of this ensemble is

$$\rho'_j = \sum_i p(i/a_j) |\psi_{ij}\rangle \langle\psi_{ij}| = \sum_i \frac{p_i P_j |\psi_i\rangle \langle\psi_i|}{p(a_j)} = \frac{P_j \rho}{tr(P_j \rho)}.$$

Evidently, when the system is in a pure state $|\psi\rangle$ then its matrix representation is $|\psi\rangle \langle\psi|$, and more general, we can show that if a system is prepared to be in states with matrix

representation ρ_i with respective probability p_i then the matrix representation of the global state is $\rho = \sum_i p_i \rho_i$.

In general, every matrix representation ρ adopted as above satisfies the following properties, and defined as *density matrix* or density operator

Definition 3.1 (Density operator)**.** *A matrix (operator) ρ is a density matrix (density operator) if and only if*

1. *ρ is a positive matrix (operator), i.e. $\forall |\psi\rangle, \langle\psi| \rho |\psi\rangle \geq 0$, and*
2. *ρ has trace equal to one - $tr(\rho) = 1$.*

Within this new language, Postulates 3.1 3.3 and 3.2 are generalized as

Postulate 3.4. *The state of any isolated system is completely described by a density operator on its state space. If the system is in state ρ_i with probability p_i then the density operator for this probabilist state is $\rho = \sum_i p_i \rho_i$.*

Postulate 3.5. *The evolution of a closed system is described by a unitary operator. Given the system in starting state ρ and a unitary operator U, the final state is then*

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

Postulate 3.6. *When measuring a system in state ρ with an observable which is a Hermitian operator $M = \sum a_i P_i, \sum_i P_i = I$, outcome a_i occurs with probability*

$$p(a_i) = tr(P_i \rho)$$

and the according output state of the system is

$$\rho_i = \frac{P_i \rho P_i}{tr(P_i \rho)}$$

An important property is that a density operator can represent infinitely many mixed states, i.e. statistical ensembles. For instance, the density operator

$$\rho = I/2 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

can be seen as a mixture $\{1/2, |i\rangle\}, i \in \{0, 1\}$ or a mixture $\{1/2, |j\rangle\}, i \in \{+, -\}$ where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. We can see later that a density operator represents also the state of a component of a composite system which is in an entangled state. No matter for which mixture a density operator stands, i.e. how it is prepared, its behavior is consistent to the laws of Postulates 3.5 and 3.6.

For the classification of ensembles which give a density matrix, Hughston et al. showed that

Theorem 3.1 ([HJW93]'s theorem)**.** *Two ensembles $\{p_i, |\psi_i\rangle\}$ and $\{q_j, |\varphi_j\rangle\}$ generate the same density matrix if and only if*

$$\sqrt{p_i} |\psi_i\rangle = \sum_j u_{ij} \sqrt{q_j} |\varphi_j\rangle ,$$

where (u_{ij}) is an unitary matrix with indexes i, j while padding some vectors 0 to the set of smaller number vectors.

3.3 Composite Systems, Entanglement and Partial Trace

In many cases, we are concerned with physical systems which are made up of distinct component systems. For describing the state of composite systems, quantum theory appeals to tensor product and issues the following postulate:

Postulate 3.7. *The state space of a composite system is the tensor product, denoted $\otimes$, of the state spaces of its component systems. If we prepare a composite system by preparing each component, indexed by $i = 1, ..., n$, in states $|\psi_i\rangle$ then the joint state of the global system is $|\psi_1\rangle \otimes ... \otimes |\psi_n\rangle$. Or, in the density operator language, if each component i is prepared in state ρ_i then the composite system is in state $\rho_1 \otimes ... \otimes \rho_n$.*

Specifically, if $\{|i\rangle\}_m$ is a basis of state space $\mathcal{H}_1$ and $\{|j\rangle\}_n$ is a basis of state space $\mathcal{H}_2$, then $\{|i\rangle \otimes |j\rangle\}_{m\times n}$ forms a basis of $m \times n$-dimension joint state space $\mathcal{H}_1 \otimes \mathcal{H}_2$. In most of cases, we can use $|ij\rangle$ for joint state $|i\rangle \otimes |j\rangle$, but not for joint state space.

A major difference of this quantum joint state space from classical counterpart is the joint superposition in the global space, i.e. given a basis $\{|i_1\rangle \otimes |j_2\rangle \otimes ...\}_{m\times n\times ...}$ (or shortly $\{|ij...\rangle\}_{m\times n\times ...}$), any superposition

$$\alpha_{11...} |11...\rangle + ... + \alpha_{mn...} |mn...\rangle , \quad \alpha_{ij...} \in \mathbb{C}$$

is also a possible state of the composite system. In principle, we can measure the composite system by an observable on the joint state space. For instance, with $M = \sum_{ij...} a_{ij...} |ij...\rangle \langle ij...|$, $a_{ij...} \in \mathbb{R}$, then outcome $a_{ij...}$ occurs with probability $|\alpha_{ij}|^2$ and the corresponding collapsed state is $|ij...\rangle$. Moreover, we can separate the components of the composite system, and measure any of the components locally. For instance, we measure only the first components with the observable $M = \sum_i b_i |i\rangle \langle i|$. The initial state of the global system may be rewritten as $\sum_i |i\rangle \otimes (\sum_{j...} \alpha_{ij...} |j...\rangle)$. Then the local measurement will project the first component to a collapsed state $|i\rangle$ with probability $p_i = \sum_{j...} |\alpha_{ij...}|^2$, and the global system is in the corresponding state $|i\rangle \otimes (\sum_{j...} \alpha_{ij...} |j...\rangle)/\sqrt{p_i}$.

Thus, this leads to a particular case that some superposition joint state $\sum_{ij...} \alpha_{ij...} |ij...\rangle$ cannot be prepared by separately preparing each component in certain states $|\psi\rangle$ and joining them as a tensor product $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ....$ With such quantum states, there is a correlation between the probability distributions of local measurements on separated components. For instance, we prepare a two-component system in a state

$$\frac{|\psi_0\rangle \otimes |\varphi_0\rangle + |\psi_1\rangle \otimes |\varphi_1\rangle}{\sqrt{2}}, \text{ for } \langle\psi_0|\,\psi_1\rangle = 0, \langle\varphi_0|\,\varphi_1\rangle$$

and separate the two components arbitrary long apart. Now we are supposed to measure the first component with an observable consisting of $|\psi_0\rangle \langle\psi_0|, |\psi_1\rangle \langle\psi_1|$, then if the first outcome occurs then the global system is collapsed to $|\psi_0\rangle \otimes |\varphi_0\rangle$, i.e. if we measure the second component with an observable consisting of $|\varphi_0\rangle \langle\varphi_0|, |\varphi_1\rangle \langle\varphi_1|$ then we receive the first outcome with certainty. Here, the action of the measurement on the first component instantly has effect on the distant second component, that makes the most fictitious characteristic of quantum theory. This phenomenon is referred to as *quantum entanglement*, discovered

and criticized by [EPR35], but confirmed by the experienced violation of variants of Bell's inequality [Bel64, TBZG98].

For describing parts of a composite system, one may seek for how to correctly describe observable quantities of these parts. The uniquely appropriate formulation found for that is the *partial trace* operator, ([NC04] - Box 2.6), defined as

$$\rho^A = tr_B(|\psi_1\rangle_A \otimes |\varphi_1\rangle_B \langle\psi_2|_A \otimes \langle\varphi_2|_B) = (\langle\varphi_2|\varphi_1\rangle)|\psi_1\rangle\langle\psi_2|.$$

Then, in the language of density operator, if a composite system in product state $\rho^{AB} = \rho_1 \otimes \rho_2$ then the reduced trace for system A is $\rho^A = tr_B(\rho_1 \otimes \rho_2) = \rho_1$. This density operator is exactly density operator state of component A. In case of entangled state, for instance

$$|\Phi+\rangle_{AB} = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$

then the partial trace for A is $\rho^A = |0\rangle\langle 0|/2 + |1\rangle\langle 1|/2$. Although this density operator is like the state of a mixture, for instance $\{1/2, |i\rangle\}, i \in \{0, 1\}$, the state of A may not exist as its state is not assigned to any real mixture. Nevertheless, the density operator ρ^A describes accurately the behavior of A according to Postulates 3.5, 3.6.

3.4 General Measurement and POVM

By coupling a system with another *ancilla system*, doing unitary dynamics and projective measurement on the ancilla, we can realized any *general measurement* ([NC04] - pages 94-95):

Postulate 3.8. *Quantum measurements are described by a collection of measurement operators $\{M_m\}$ acting on the state space of the system being measured. This collection satisfies the completeness: $\sum_m M_m^\dagger M_m = I$, the identity operator.*

If the state of the system before the measurement is $|\psi\rangle$ then outcome m occurs with probability

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

and after the measurement, when m occurs, the system is in state

$$\frac{M_m|\psi\rangle}{p(m)}$$

Or in the density operator language, if the initial state is ρ then

$$p(m) = tr(M_m^\dagger M_m \rho)$$

and the corresponding final state is

$$\rho_m = \frac{M_m^\dagger \rho M_m}{\sqrt{p(m)}}$$

When we are only interested in the measurement statics, not the post-measurement state of the system being measured, it suffices to abbreviate the measurement operator as Positive Operator-Valued (POV)

$$E_m = M_m^\dagger M_m, \text{ for } M_m \text{ being general measurement operators.}$$

The measurement of a system in state $|\psi\rangle$ will output m with probability

$$p_m = \langle\psi| E_m |\psi\rangle .$$

Any POV measurement (POVM) is then defined as a collection of *positive operators* $\{E_m\}$, i.e. $\forall m, |\psi\rangle , \langle\psi| E_m |\psi\rangle \geq 0$, such that $\sum_m E_m = I$. This formalism is simpler than the one for general measurements and sufficient to determine the probabilities of different outcomes in a general measurement.

3.5 Non-Cloning and Distinguishability

In many circumstances, it may happen that we have to identify or guess the state of a single quantum system, prepared to be in a state from a set $\{\rho_b\}$ assigned some *a priori* probabilities $\{p_b\}$, i.e. the statistical ensemble $\{p_b, \rho_b\}$. We will see that the distinguishability of quantum states is a fundamental measure for the security of quantum cryptographic protocols.

A crucial property of quantum system is that we cannot reliably copy an arbitrary quantum state [WZ82]. Indeed, suppose we have such a copying machine, which couples the system that we want to copy its state $|\psi\rangle$ with an equivalent system initialized in a certain state $|e\rangle$, and does a quantum dynamics over the composite system to have the second system in the desired state $|\psi\rangle$. In the quantum language, this dynamics is a unitary operator over the product state space:

$$U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle .$$

Thus, for any two different states $|\psi_1\rangle , |\psi_1\rangle$:

$$U(|\psi_1\rangle \otimes |e\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle , \quad U(|\psi_2\rangle \otimes |e\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle .$$

And, by the linearity of quantum operators, if we introduce a state $|\psi'\rangle = a |\psi_1\rangle + b |\psi_2\rangle$ then the output state is

$$U((a |\psi_1\rangle + b |\psi_2\rangle) \otimes |e\rangle) = U(a |\psi_1\rangle \otimes |e\rangle + b |\psi_2\rangle \otimes |e\rangle) = a |\psi_1\rangle \otimes |\psi_1\rangle + b |\psi_2\rangle \otimes |\psi_2\rangle$$

which is not the desired result $|\psi'\rangle \otimes |\psi'\rangle$ that the copying action would have made. Moreover, as the unitary operator preserves the inner product:

$$\begin{aligned} \langle e| \otimes \langle\psi_1| \psi_2\rangle \otimes |e\rangle &= \langle e| \otimes \langle\psi_1| U^\dagger U |\psi_2\rangle \otimes |e\rangle \\ \Rightarrow \langle e| \otimes \langle\psi_1| \psi_2\rangle \otimes |e\rangle &= \langle\psi_1| \otimes \langle\psi_1| \psi_2\rangle \otimes |\psi_2\rangle \\ \Leftrightarrow \langle\psi_1| \psi_2\rangle &= \langle\psi_1| \psi_2\rangle^2 \end{aligned}$$

that can only happen when either $\langle\psi_1|\,\psi_2\rangle = 0$ or $\langle\psi_1|\,\psi_2\rangle = 1$, i.e. $|\psi_1\rangle, |\psi_2\rangle$ are either orthogonal or identical. Thus, we cannot copy quantum states belonging to a set of non-orthogonal states.

Evidently, if we are given a system in a state belonging to a set or orthogonal states $\{|v_i\rangle\}$, we can measure it with a projective measurement $\{P_i = |v_i\rangle\langle v_i|\}$ and prepare a new system in state $|v_i\rangle$ if outcome i occurs.

Conforming to that, two non-orthogonal states cannot be reliably distinguished by any measurement. One see that, for distinguishing quantum states, one must use a certain measurement, which is in general a POVM $\{E_i\}$, and one may distinguish them based on the probability distribution of outcomes for each prepared state [Fuc95].

Suppose that we are provided a quantum system in one of two states ρ_1, ρ_2 with which the POVM outputs i with respective probabilities p_i, q_i. The distinguishability can be then measured as the distance between probability distributions p_i, q_i. A convenient measure of distance is the *fidelity*

$$F(p_i, q_i) = \sum_i \sqrt{p_i q_i}.$$

We see that when $F(p_i, q_i) = 1$, the two distributions are identical, i.e. we cannot distinguish them, and when $F(p_i, q_i) = 0$ then for all outcomes i one can reliably distinguish p_i, q_i because there must be either $p_i = 0$ or $q_i = 0$. And so, the distinguishability of two quantum states can be measured by the fidelity of *the best measurement*, i.e.

$$F(\rho_1, \rho_2) = \min_{\{E_i\}} F(p_i, q_i)$$

It is shown that [NC04]

$$F(\rho_1, \rho_2) = tr\sqrt{\rho_1^{1/2}\rho_2\rho_1^{1/2}}$$

The first proposal for quantum fidelity, due to Jozsa, was the square of the above commonly used fidelity, i.e. $(tr\sqrt{\rho_1^{1/2}\rho_2\rho_1^{1/2}})^2$ [Joz94].

Therefore, provided two non orthogonal states $|\psi_1\rangle, |\psi_2\rangle$, $F(|\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|) = |\langle\psi_1|\,\psi_2\rangle| > 0$, we cannot reliably distinguish them.

Another usual measure of distinguishability is the mutual information that the outcomes of the measurement reveal about the initial state. For a POVM $\{E_b\}$, the probability of outcome b is

$$p(b) = \sum_i p_i tr(\rho_i E_b) = tr(\rho E_b)$$

where $\rho = \sum_i p_i\rho_i$ is the density matrix for the ensemble $\{p_i, \rho_i\}$. Besides, the probability of outcome b when the system is prepared in state ρ_i is

$$p_i(b) = tr(\rho_i E_b).$$

Then the mutual information [Sha48, CT91] with the POVM $\{E_b\}$ is

$$I(i; b) = H(b) - \sum_i p_i H(b/i)$$

where $H(b) = \sum_b p(b) \log p(b)$ and $H(b/i) = \sum_b p_i(b) \log p_i(b)$. This amount of accessible information is bounded by Holevo's inequality:

$$I(i;b) \leq S(\rho) - \sum_i p_i S(\rho_i)$$

where $S(.)$ is Von Neumann entropy function of a density matrix:

$$S(\rho) = -tr(\rho \log \rho). \tag{3.1}$$

Conformally, the mutual information is sufficient to reveal the identity of the prepared state, $I(i;b) = H(i)$, when the subspaces expanding ρ_i's eigenstates are pairwise orthogonal. In contrast, if $S(\rho) - \sum_i p_i S(\rho_i) < H(i)$, normally caused by the non-orthogonality of $\{\rho_i\}$ then there is no measurement $\{E_b\}$ which helps to perfectly infer the value of i from the quantum codes.

3.6 Bipartite State: Schmidt Decomposition and Purification

This dissertation is primarily concerned with composite systems made up of two major components lying at users' locations of two-party protocols. This kind of composite systems is specifically named bipartite systems whose states are described in a bipartite state space.

Two properties of great importance for bipartite systems are the Schmidt decomposition and purification.

Theorem 3.2 (Schmidt decomposition)**.** *Suppose $|\psi\rangle$ is a pure state of the composite system AB where the state spaces $\mathcal{H}_A, \mathcal{H}_B$ are of dimensions m, n respectively. Then there exist an orthonormal vector set $\{|u_1\rangle, ..., |u_r\rangle\}$ of $\mathcal{H}_A$ and an orthonormal orthonormal set $\{|v_1\rangle, ..., |v_r\rangle\}$ with some $r \leq \min\{m, n\}$ such that*

$$|\psi\rangle = \sum_{i=1}^{r} \lambda_i |u_i\rangle |v_i\rangle ,$$

where λ_i are positive real numbers, named Schmidt-coefficients.

Proof. Suppose ρ^A is the reduced density matrix of $|\psi\rangle$ for system A:

$$\rho^A = tr_B(|\psi\rangle \langle\psi|).$$

This matrix is diagonalizable with positive eigenvalues p_i and stands for an ensemble of its $r \leq \min\{m, n\}$ eigenstates $\{p_i, |u_i\rangle\}$. We can add to this ensemble some orthonormal states $|u_i\rangle, i = r+1, ..., m$ (with probability 0). These eigenstates form an orthonormal basis of $\mathcal{H}_A$. Then, there exist vectors $|\varphi_i\rangle$ in $\mathcal{H}_B$ such that

$$|\psi\rangle = \sum_{i=1}^{m} |u_i\rangle |\varphi_i\rangle$$

As, $\rho^A = tr_B(|\psi\rangle\langle\psi|)$, it musts hold that $\langle\varphi_i|\varphi_j\rangle = 0$ for $i \neq j$, $\langle\varphi_i|\varphi_i\rangle = 1$ for $i = 1, ..., r$ and $\langle\varphi_i|\varphi_i\rangle = 0$ for $i = r+1, ..., m$.

Thus, we can find the orthonormal states $|v_i\rangle = \lambda_i |\varphi_i\rangle$ with $\lambda_i > 0$ and

$$|\psi\rangle = \sum_{i=1}^{r} \lambda_i |u_i\rangle |\varphi_i\rangle .$$

Returning to the diagonal form of ρ^A, we notice that $p_i = \lambda_i^2$. □

With this decomposition of bipartite states, Theorem 3.1 implies an important corollary for *generating ρ-ensemble at space-like separation*, which leads directly to the *no-go theorem for bit commitment* of Mayers, Lo and Chau [May97, LC97]:

Theorem 3.3 (theorem for bit commitment)**.** *Suppose $|\psi_0\rangle, |\psi_1\rangle$ are two pure states of a bipartite system AB satisfying that the reduced partial traces for B are identical:*

$$tr_A(|\psi_0\rangle\langle\psi_0|) = tr_A(|\psi_1\rangle\langle\psi_1|).$$

Then there exists a local unitary transformation acting on the state space of A, U_A, that maps $|\psi_0\rangle$ into $|\psi_1\rangle$:

$$U_A |\psi_0\rangle_{AB} = |\psi_1\rangle_{AB}$$

Proof. (Sketch) - Let the Schmidt decompositions of $|\psi_0\rangle$, $|\psi_1\rangle$ be

$$|\psi_0\rangle = \sum_{i=1}^{r} \lambda_i |e_i\rangle |f_i\rangle , |\psi_1\rangle = \sum_{j=1}^{r'} \lambda'_j \left|e'_j\right\rangle \left|f'_j\right\rangle .$$

As $tr_A(|\psi_0\rangle\langle\psi_0|) = tr_A(|\psi_1\rangle\langle\psi_1|)$, it musts hold that $r = r'$ and $\forall i = j, \lambda_i = \lambda_j, |f_i\rangle = \left|f'_j\right\rangle$. Thus, there exists a unitary transformation on $\mathcal{H}_A$ that transforms the orthonormal set $\{e_i\}$ into $\{|e'_i\rangle\}$, and hence $|\psi_0\rangle$ into $|\psi_0\rangle$. □

On the other hand, the purification assumes that for the state ρ of a system A, we can introduce another system B and prepare a pure state $|\psi\rangle$ for the composite system AB such that the reduced partial density matrix for A is the same as ρ:

$$tr_B(|\psi\rangle\langle\psi|) = \rho$$

Notice that, from the Schmidt decomposition, cf. Theorem 3.2, it suffices to take $\mathcal{H}_B = \mathcal{H}_A$. There may be many purification of a particular density matrix ρ.

Moreover, the relation between a density matrix and its purification states is stated by Uhlmann's theorem [Joz94]

Theorem 3.4 (Uhlmann's theorem)**.** *Suppose ρ_1, ρ_2 are two density operators acting on a same state space then*

$$F(\rho_1, \rho_2) = \max |\langle\psi_1|\psi_2\rangle|$$

where the maximum is taken over all purifications $|\psi_1\rangle$ of ρ_1 and $|\psi_2\rangle$ of ρ_2.

Indeed, the proofs of Uhlmann's theorem gave a strengthen version of this theorem ([NC04] - exercise 9.15) [Joz94]:

Theorem 3.5 (strengthen Uhlmann's theorem)**.** *Suppose ρ_1, ρ_2 are two density operators acting on a same state space, and $|\psi_1\rangle$ is a purification of ρ_1 then*

$$F(\rho_1, \rho_2) = \max |\langle\psi_1|\psi_2\rangle|$$

where the maximum is taken over all purifications $|\psi_2\rangle$ of ρ_2, and there exists a purification $|\psi_2\rangle$ realizing the maximum.

3.7 Quantum Mechanical Processing of Information

Finally, the laws of quantum physics can be used for information processing as in Figure 3.1: information are represented by quantum states, processed by quantum operators, and finally observed by human via measurements.

Similarly to the domain of classical information, the elementary unit of quantum information is a quantum bit, named *qubit*, which is the state of a single physical system of 2-dimension state space $\mathcal{H}_2$. Normally, a standard orthonormal basis is selected with two orthonormal qubits $\{|0\rangle, |1\rangle\}$, and any qubit is expressed as a superposition $a|0\rangle + b|1\rangle$. Physically, a qubit can be carried out by the polarization of a photon, the spin of an electron, or any two-state system ... [Pre].

Moreover, quantum information inherits the features of quantum mechanics, issuing various important results. The emergence of quantum information processing has the most noticeable impacts to the domain of Cryptology, for both Cryptography and Cryptanalysis.

Quantum Computing

Quantum computing is primarily concerned with the the design of quantum algorithms for desired computations. The most referred as standard quantum computational model is the circuit model which consists of three stages: (i) preparing a quantum system in state $|0\rangle$; (ii) applying a unitary evolution to the initial state; (iii) reading out the final result with measurements [NC04]. Though there exist some other equivalent computational models such as measurement-based computation model [RB01, Nie03], quantum adiabatic computation [FGGS00, vDMV01, Rol04, AvDK$^+$04], we will primarily use the standard quantum circuit model in the sequel.

It is stated that any quantum unitary transformation on an n-qubit system can be decomposed into one-qubit unitary rotations and two-qubit controlled not (CNOT) gates [NC04]. The complexity of a quantum transformation is then measured by the number of these primitive gates used for building it.

Any sequence of qubits is then characterized by the product of their state spaces, $\mathcal{H}_2 \otimes ... \otimes \mathcal{H}_2$. Thus, if a classical message of n bits can take one of 2^n values $x \in \{0,1\}^n$, a quantum message of n qubits can be in any of infinitely many states $\sum_{x\in\{0,1\}^n} c_x |x\rangle, c_x \in \mathbb{C}$. The information processing algorithms are realized by unitary quantum dynamics. Thus, by the linearity, if we introduce a superposition of inputs to a unitary U then we can get

a superposition of processed counterparts: $U(\sum_{x\in\{0,1\}^n} c_x |x\rangle) = \sum_{x\in\{0,1\}^n} c_x U |x\rangle$. This property makes the fictitious parallelism of quantum information processing , exploited to build robust quantum algorithms [NC04].

This new discipline has led to outstanding results, ever gainable in the classical computing models [Sho94, Gro96]. This progress has most impact on the field of Cryptanalysis: Shor's quantum factoring algorithm would breaks down the widely used RSA and related systems; Grover's search algorithm would speed up the breaking of secret keys [Gro96].

Quantum Communication

In another direction, the communication of quantum information also reveals advantageous features.

The non-copiability and non distinguishability of non orthogonal states can help to build quantum communication channel which help to implement unconditionally secure protocols, imposible with trivial classical counterpart, for exchanging secret keys [BB84, Eke91, Ben92].

Besides, the special correlation between the states of distantly separated quantum systems, known as quantum entanglement, provides significant reduction of the cost of communication in distributed computations [BW92, SvD00, BCvD]. Quantum entanglement also helps to transfer an unknown quantum state by sending only classical information [BBC$^+$93].

Chapter 4

Noisy Channels, Quantum Conjugate Channel, and The No-go Theorems

As shown in the Chapter 2, general secure two-party computations can be implemented, solely based on oblivious transfer. In turn, oblivious transfer cannot be classically built from scratch, i.e. without any assumption [Kil88]. Nevertheless, this primitive becomes an intermediate layer, a term borrowed from the field of computer network engineering, that separates well the applications from specific cryptographic assumptions, such as modern computational complexity assumptions. This relaxing encouraged researchers to investigate whether they can make the security of protocols better, based on other assumptions than computational complexity ones.

The main stream of these investments is seeking for realistic noisy channels that could implement oblivious transfer protocols. The implementation is based only on information theory that carries a provable *unconditional* security, evidently depending on assumptions about noise models.

In one direction, these investments relax the assumption of standard oblivious transfers, Rabin OT and one-out-of-two OT. This weakening action may cover a larger class of possible noisy models [CK88, Cré97, DKS99, KM01, SW02, CMW04, Mor05].

In the other direction, one would find out practically physical channels that match the theoretical assumptions. Since the introduction of quantum mechanics into the field of communication and cryptography [Wie83], the successful implementation of key exchange schemes [BB84, Eke91, Ben92] with provable unconditional security [LC99, SP00] has encouraged researchers to seek for quantum unconditionally secure bit commitment and oblivious transfer [CK88, BBCS92, BCJL93]. Much interest aimed to exploit the uncertainty principle and the non-cloning property to implement wanted noisy channels for oblivious transfer [CK88, BBCS92]. However, this intention was rejected by a no-go theorem of Mayers and Lo & Chau, which was first discovered for quantum bit commitment protocols [May97, LC97] and then for quantum oblivious transfer protocol [Lo97].

The material of this chapter concerns a review of the two mentioned research directions

and Mayer's, Lo's & Chau's no-go theorems.

4.1 A General Definition of Oblivious Transfer

Even though one-out-of-two oblivious transfer and Rabin's oblivious transfer are equivalent [Cré88], the former is more convenient to use and considered as the standard version of oblivious transfers. We will shortly name it "oblivious transfer" while Rabin's version will be named "Rabin OT".

Simply speaking, by definition, OT is a primitive where Alice has two secret bits b_0, b_1 and Bob can choose to get one but not both while Alice cannot know Bob's choice. In terms of information theory and probabilities, we usually work with non-ideal oblivious transfers as oblivious transfer protocols provided characterizing parameters.

Definition 4.1. *An oblivious transfer protocol is a transmission scheme where Alice has two secret bits b_0, b_1 to send to Bob who has a choice c to get the bit b_c. The scheme assumes three non-zero values:*

- *Correctness P_C: the probability that Bob gets b_c when Alice and Bob are honest.*
- *Alice's privacy H_B: the final minimal remaining uncertainty of Bob about b_{1-c} whatever his strategy when Alice is honest.*
- *Bob's privacy H_A: the final minimal remaining uncertainty of Alice about c whatever her strategy when Bob is honest.*

We see that an ideal oblivious transfer protocol has $P_C = 1, H_B = 1, H_A = 1$. In an asymptotic manner, we can have unconditional but non-ideal oblivious transfer with P_C, H_B, H_A asymptotically close to 1, depending on some parameter N.

4.2 Building Oblivious Transfer from Noisy Channels

4.2.1 Oblivious Transfer as Erasure Channels

The original version of oblivious transfer protocol, proposed by Rabin [Rab81], is simply a *Binary-Symmetric Erasure Channel* with erasure probability 1/2:

Definition 4.2. *BSEC(r) $\Leftrightarrow$ Rabin OT(r)*

1. *Alice sends r.*
2. *Bob receives* $r' = \begin{cases} r & \text{with probability } 1/2, \\ \perp & \text{with probability } 1/2. \end{cases}$

where $\perp$ is the erasure out put symbol.

This erasure channel can implement the chosen one-out-of-two oblivious transfer, following Crepeau's reduction scheme [Cré88]:

Protocol 4.1. *$BSEC \rightarrow OT(b_0, b_1)(c)$*

1. *Alice picks $3n$ random bits r_i, $i = 1, ..., 3n$, and sends to Bob via the BSEC. Bob receives r'_i, Δ_i*
2. *Bob makes two disjoint index sets I_0, I_1, $|I_0| = |I_1| = n$, such that $\Delta_i = 0$ for all $i \in I_0$, and announces (I_c, I_{1-c}) to Alice.*
3. *Alice computes $\hat{b}_0 = \left(\bigoplus_{i \in I_c} r_i\right) \oplus b_0$, $\hat{b}_1 = \left(\bigoplus_{i \in I_{1-c}} r_i\right) \oplus b_1$ and sends to Bob.*
4. *Bob computes $b_c = \left(\bigoplus_{i \in I_0} r'_i\right) \oplus \hat{b}_c$*

Roughly speaking, based on the Law of Large Numbers, the correctness of Protocol 4.1 can be hold as Bob receives in average $3n/2$ bits r_i without errors with large value of n. So Bob can make n indexes I_0 with complete knowledge of r_{I_0} for decoding $\hat{b}_c$. Nevertheless, Bob cannot set $2n$ indexes for getting complete knowledge of $r_{I_0}.r_{I_1}$, and thus one of b_0, b_1 must can not be learned.

4.2.2 General Binary Symmetric Erasure Channel

Relaxing the security assumptions, we can have an extended version of imperfect binary symmetrical erasure channel:

Definition 4.3. *(φ, φ', p_g)-BSEC*

1. *Alice sends r.*
2. *Bob receives (r', Δ) with $\Delta = \begin{cases} 0 & \text{with probability } p_g, \\ 1 & \text{with probability } 1 - p_g, \end{cases}$*

where Δ is a symbol denoting the erasure status of the channel. The error rate in the non-erased case is φ, i.e. $p(r' \neq r / \Delta = 0) = \varphi$ and the error rate in the erased case is significantly greater, bounded by φ': $1/2 \geq p(r' \neq r / \Delta = 1) \geq \varphi' > \varphi$.

Inspired from Crépeau's reduction [Cré88], with help of appropriate error-correcting codes and privacy amplification algorithms, we can implement an oblivious transfer protocol with this imperfect erasure channels [Cré97, CMW04]:

Protocol 4.2. *(φ, φ', p_g)-BSEC $\rightarrow$ $OT(b_0, b_1)(c)$*

1. *Alice picks N random bits r_i, $i = 1, ..., 2N$, and sends to Bob via the (φ, β, p_g)-BSEC. Bob receives r'_i, Δ_i*
2. *Bob makes two disjoint index sets I_0, I_1, $|I_0| = |I_1| = n$, such that $\Delta_i = 0$ for all $i \in I_0$, and announces (I_c, I_{1-c}) to Alice.*
3. *Alice computes and sends $(s_0 = syn(r_{I_c}), s_1 = syn(r_{I_{1-c}}))$ to Bob.*
4. *Alice picks a sequence of n random bits m and sends to Bob.*

5. *Alice computes and sends* $(\hat{b}_0 = k_0 \oplus b_0, \hat{b}_1 = k_1 \oplus b_1)$ *to Bob, with* $k_0 = (r_{I_c} \odot m)$, $k_1 = (r_{I_{1-c}} \odot m)$.

6. *Bob uses* s_c *to correct errors in* r'_{I_0}, *computes* $k_c = (r'_{I_0} \odot m)$ *and* $b_c = k_c \oplus \hat{b}_c$.

The intuition behind Protocol 4.2 is that Bob can correct all errors in r_{I_0} when he is honest while, even though Bob is dishonest, the average error rate in both $r_{I_0}.r_{I_1}$ is significantly greater and so a significant amount of error bits remains in at least one of $r_{I_i}, i \in \{0,1\}$. The distribution of error rates received by Bob can be illustrated as in Figure 4.1.

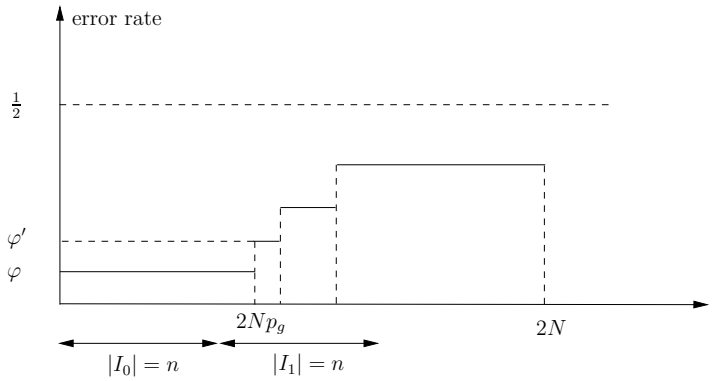

Figure 4.1: Distribution of error rates received by Bob

In this construction, P_C is the probability that honest Bob, who makes I_0 as the index subset with the best average error rate, can correct all of the errors in r'_{I_0} with $syn(r_{I_0})$. H_B is the uncertainty of k_{1-c} after the error correction and the privacy amplification phases, even though Bob is free to set I_0, I_1,

$$H_B = \max_{i=0,1} \left(\sum_{m \in 2^n} p(m) H(r_{I_i} \odot m / r'_{I_i}, syn(r_{I_i}), m) \right).$$

We can have both P_C, H_B asymptotically close to 1 with large values of N and an appropriate choice of n and the error correcting code [CMW04].

In Protocol 4.2, we choose $n = (p_g + \beta)N$ with $0 < \beta < p_g$. As $n < p_g 2N$ then Bob can almost set I_0 with error rate φ in r'_{I_0}. Simply speaking the missing information of r_{I_0} is $H(r_{I_0}/r'_{I_0}) = nh(\varphi)$. Then Alice sends s_0, s_1 each of which contains at least $nh(\varphi)$ bits of information. Meanwhile, as $2n > p_g 2N$, $r'_{I_0}.r'_{I_1}$ accumulates some received bits an error rate significantly greater than φ. The missing information of $r_{I_0}.r_{I_1}$ is

$$H(r_{I_0}.r_{I_1}/r'_{I_0}.r_{I_1}) \geq p_g 2N h(\varphi) + (2n - p_g 2N) h(\varphi')$$

Then the coding theory permits to use codes with

$$|s_0| = |s_1| = H(r_{I_0}/r'_{I_0}) + \frac{H(r_{I_0}.r_{I_1}/r'_{I_0}.r'_{I_1}) - 2H(r_{I_0}/r'_{I_0})}{4} = (n + p_g N)h(\varphi) + (n - p_g N)h(\varphi')$$

for efficiently correct r'_{I_0} while there remain at least $(n-p_gN)(h(\varphi')-h(\varphi))/2$ bits of missing information in one of r'_{I_0}, r'_{I_1}. Then, the privacy amplification operation $(r_{I_i} \odot m), i \in \{0,1\}$ enhances the security that prevents Bob from learning both b_0, b_1.

Besides, Bob's selection of index sets I_0, I_1 depends only on the probability distribution of Δ_i that is uniform for all index $i = 1, ..., N$. Thus, Alice cannot distinguish I_0, I_1 to gain information about c.

4.2.3 Non-trivial Discrete Memoryless Channel

A discrete memoryless channel (DMC) is a statistical model describing the communication medium with discrete input alphabets $\mathcal{X} = \{x_1, .., x_n\}$, output alphabets $\mathcal{Y} = \{y_1, .., y_m\}$, and the current output received by the receiver depends only on the current input of the emitter, corresponding to a probability distribution $P_{X/Y}$.

Informally speaking, a DMC is non-trivial if it cannot be decomposed into separate sub-channels each of which has capacity 0 or 1. [CMW04] states a special character of non-trivial DMC that

Theorem 4.1 (CMW theorem on DMC)**.** *There exist $x_1, x_2 \in \mathcal{X}$ such that*

1. $P_{Y/X=x_1} \neq P_{Y/X=x_2}$*;*
2. *there exist $y \in \mathcal{Y}$ such that $P_{Y/X=x_1}(y) > 0, P_{Y/X=x_2}(y) > 0$;*
3. *let, for $\lambda, \mu_i \in [0,1]$,*

$$\lambda P_{Y/X=x_1} + (1-\lambda) P_{Y/X=x_2} = \sum_i \mu_i P_{Y/X=x_i}$$

then $\mu_i > 0$ implies that $P_{Y/X=x_i} = \tau P_{Y/X=x_1} + (1-\tau) P_{Y/X=x_2}$

The first and the second properties assume that there exists an input pair x_1, x_2 such that we have some possibility to distinguish them but not conclusively. Besides, the third property assumes that if the sender uses some other input symbols to simulate a random input that takes only x_1, x_2 then these fake symbols must be redundant, and cannot help the sender. Nevertheless, if the sender is supposed to use x_1, x_2, and if he does not respect by using some non-redundant symbols, then the output probability distribution is modified, and can be detected by statistics.

A special case of DMC is binary Symmetric Channel. This kind of noisy channels has been considered very early in [CK88, Cré97] for building oblivious transfer. ϵ-BSC is denoted for a binary symmetric channel with error rate ϵ, i.e. it flips the bit sent on it with probability ϵ:

$$\epsilon - BSC(x) = \begin{cases} \overline{x} & \text{with probability } \epsilon \\ x & \text{with probability } 1-\epsilon. \end{cases}$$

We have a non-trivial BSC channel when its capacity is neither 1 or 0, i.e. when $\epsilon \notin \{0, 1/2, 1\}$. We suppose that $0 < \epsilon < 1$ because when $\epsilon > 1/2$ we can flip the output and have the same channel with error rate $1-\epsilon$.

Building Binary Symmetric Erasure Channel

Let $x_1, x_2 \in \mathcal{X}$ be two input of the DMC satisfying the above properties, cf. Theorem 4.1, we can implement a binary symmetric erasure channel as follows:

Protocol 4.3. $P_{Y/X} \to (\varphi, \varphi', p_g) - BSEC(r)$

1. *Alice encodes* $r = 0$ *as* $x_1.x_2$, $r = 1$ *as* $x_2.x_1$ *and sends them via the DMC.*

2. *Bob outputs* $\begin{cases} r' = 0, \Delta = 0 & \text{if } y_1.y_2 \text{ is received,} \\ r' = 1, \Delta = 0 & \text{if } y_2.y_1 \text{ is received,} \\ r' = \text{best guess}, \Delta = 1 & \text{otherwise.} \end{cases}$

   where y_1, y_2 are chosen to minimize the error rate:

$$\varphi = \min_{(y^0, y^1) \in \mathcal{Y} \times \mathcal{Y}} \frac{P_{Y/X=x_1}(y^1) P_{Y/X=x_2}(y^0)}{P_{Y/X=x_1}(y^0) P_{Y/X=x_2}(y^1) + P_{Y/X=x_1}(y^1) P_{Y/X=x_2}(y^0)} \tag{4.1}$$

And p_g is the probability of receiving this output pair which minimizes the error rate:

$$p_g = P_{Y/X=x_1}(y_1) P_{Y/X=x_2}(y_2) + P_{Y/X=x_1}(y_2) P_{Y/X=x_2}(y_1).$$

If there are many pairs (y_1, y_2) which give the same error rate φ, we should consider all of them as good pairs, and p_g is the sum of the probabilities of receiving these pairs. φ' is then defined as the second lowest error rate realized by another output symbol pair (y_1', y_2').

Crépeau [Cré97] had also proposed an equivalent construction, using repetition code for BSC:

Protocol 4.4. $\epsilon - BSC \to (\varphi, \varphi', p_g) - BSEC(r)$ *[Cré97]*

1. *Alice encodes* r *by the repetition code* $r.r$*, and sends the two encoding bits to Bob via the* ϵ*-BSC.*

2. *If Bob receives* $r'.r'$ *then he outputs* $r', \Delta = 0$*; else he outputs* $\Delta = 1$ *and* r' *as random (or his best guess of* r*).*

Building Oblivious Transfer

In the above construction of BSEC from DMC and BSC, Alice can affect the probability that Bob considers as having got the good bit by violating the coding convention:

1. Alice sends forbidden input symbols $x \notin \{x_1, x_2\}$ in the implementation of BSEC from DMC.

2. Alice uses x_1, x_2 but does not respect the conventional encoding, i.e. she sends $x_1.x_1$ or $x_2.x_2$. For instant, in the implementation from BSC, cf. Protocol 4.4, Alice sends $r.\overline{r}$:

$$p_g' = 2\epsilon(1 - \epsilon) \neq p_g$$

If we use these BSEC and Protocol 4.2 to implement an oblivious transfer, Alice can change p_g for different positions $i = 1, ..., 2N$ and have some possibility to distinguish I_c, I_{1-c} considering that the sending of r_i via BSEC with a higher probability of non-erasure will make i have more chance to be put in I_c.

Fortunately, Theorem 4.1 states that the forbidden input symbols would cause a probability distribution on output symbols different from the determined pair x_1, x_2. Similarly, if Alice uses x_1, x_2 but does not respect the conventional encoding, the distribution of output (y_1, y_2) also changes. These cheating behaviors can be statistically detected in a more advanced scheme that requires a large number of executions of Protocol 4.2 [Cré97, CMW04]:

Protocol 4.5. *$DMC \to OT(b_0, b_1)(c)$*

1. *Alice picks M random bits $b_{1,0}, ..., b_{M,0}$ and sets $b_{l,1} = b_0 \oplus b_1 \oplus b_{l,0}$ for $l = 1, ..., M$.*
2. *Bob picks M random bits $c_1, ..., c_M$.*
3. *For $l = 1, ..., M$, Alice and Bob run Protocol 4.2 that use the BSEC built from the DMC (cf. Protocol 4.3 or 4.4) with that Bob gets b'_l with his choice c_l.*
4. *Bob checks the statistics of the channel and aborts if Alice cheats.*
5. *Bob sends $c' = \bigoplus_{l=1}^{M} c_l \oplus c$*
6. *Alice computes $\hat{b}_0 = \bigoplus_{l=1}^{M} b_{l,c'} \oplus b_0$, $\hat{b}_1 = \bigoplus_{l=1}^{M} b_{l,(1-c')} \oplus b_1$ and sends to Bob.*
7. *Bob computes $b_c = \bigoplus_{l=1}^{M} b'_l \oplus \hat{b}_c$.*

The idea is that Alice must attack all of M executions of Protocol 4.2 by violating the coding convention to learn c. In that case, Bob can detect Alice's dishonesty with statistics on outputs [Cré97, CMW04].

4.3 Oblivious Transfers from Quantum Conjugate Channel

4.3.1 Quantum Conjugate Coding Channel

Quantum conjugate coding was first proposed by Wiesner for implementing an application, named multiplexing channel, similar to oblivious transfer [Wie83].

We denote $\{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |\times\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$. The two bases, rectangular basis $\{|0\rangle, |1\rangle\}$ and diagonal basis $\{|+\rangle, |\times\rangle\}$, are said to be conjugate in the sense that the measurement of a basis state in the other basis gives a maximally random output and vice-versa, e.g. the measurement of $|+\rangle$ in the rectangular basis outputs $|0\rangle$ or $|1\rangle$ with probability 1/2.

Protocol 4.6. *QCC(r)*

1. *Alice randomly chooses one of two conjugate bases: rectangular basis $\{|0\rangle, |1\rangle\}$ or diagonal basis $\{|+\rangle, |\times\rangle\}$.*

2. *Alice encodes the bit r by the corresponding basis state: $|0\rangle$ or $|+\rangle$ if $r = 0$; $|1\rangle$ or $|\times\rangle$ if $r = 1$. Alice sends the encoding state to Bob.*

3. *Bob randomly chooses the rectangular or diagonal basis to measure the incoming state. Bob outputs r'.*

4.3.2 Quantum Binary Symmetric Erasure Channel

This scheme does not implement correctly an oblivious transfer protocol. It would rather be a Binary-Symmetric Channel with error rate equal to 1/4. Wiesner suggested also to use some error-correcting codes to establish a scheme similar to what we call today one-out-of-two string oblivious transfer. However Wiesner's construction was not complete.

A modification of Wiesner's conjugate coding channel provides a binary symmetric erasure channel, used to implement quantum oblivious transfer [CK88, BBCS92, Cré94].

Protocol 4.7. *QCC → BSEC(r)*

1. *Alice randomly chooses one of two conjugate bases: rectangular basis $\{|0\rangle, |1\rangle\}$ or diagonal basis $\{|+\rangle, |\times\rangle\}$.*

2. *Alice encodes the bit r by the corresponding basis state: $|0\rangle$ or $|+\rangle$ if $r = 0$; $|1\rangle$ or $|\times\rangle$ if $r = 1$. Alice sends the encoding state to Bob.*

3. *Bob randomly chooses the rectangular or diagonal basis to measure the incoming state. Bob outputs r'.*

4. *Alice announces her basis to Bob.*

5. *If Bob's basis matches Alice's one, Bob outputs $\Delta = 0$, otherwise Bob outputs $\Delta = 1$.*

4.3.3 Quantum Oblivious Transfer based on Bit Commitment

We state that Protocol 4.7 is no more an erasure channel in case Bob can store the quantum state and do the measurement after having known Alice's basis. It was suggested to use a bit commitment protocol to force Bob doing the measurement before the announcement of Alice's basis. The canonical form of bit-commitment-based quantum oblivious transfer is:

Protocol 4.8. *BC and QCC → $OT(b_0, b_1, c)$*

1. *Alice picks N random bits r_i, and N random bases $\theta_i \in \{rectangular, diagonal\}$, $i = 1, ..., N$. Alice encodes r_i by the corresponding state in basis θ_i, and sends the quantum states to Bob.*

2. *For each i^{th} incoming state, Bob randomly chooses a basis $\theta'_i \in \{rectangular, diagonal\}$ to measure it, and output r'_i.*

3. *Bob makes the commitment of θ'_i, r'_i for all $i = 1, ..., N$ to Alice.*

4. *Alice randomly chooses an index set $T, |T| = t$, and sends to Bob.*

5. *Bob opens the commitment of* θ'_i, r'_i *for all* $i \in T$. *Alice tests if* $\theta'_i = \theta_i \Rightarrow r'_i = r_i$ *fails then aborts.*

6. *Alice announces* θ_i *for all* $i \in I = \{1, ..., N\} \setminus T$ *to Bob. Bob outputs* $\Delta_i = 0$ *if* $\theta_i = \theta'_i$, $\Delta_i = 1$ *otherwise.*

7. *Bob makes two disjoint index sets* $I_0, I_1 \subset I$, $|I_0| = |I_1| = n$, *such that* $\Delta_i = 0$ *for all* $i \in I_0$, *and announces* (I_c, I_{1-c}) *to Alice.*

8. *Alice computes* $s_0 = syn(r_{I_0}), s_1 = syn(r_{I_1})$ *and sends to Bob.*

9. *Alice picks a sequence of* n *random bits* m *and sends to Bob.*

10. *Alice computes* $\hat{b}_0 = (r_{I_0} \odot m) \oplus b_0$, $\hat{b}_1 = (r_{I_1} \odot m) \oplus b_1$ *and sends to Bob.*

11. *Bob uses* s_c *to correct errors in* r_{I_c}, *and computes* $b_c = (r_{I_c} \odot m) \oplus \hat{b}_c$

The security against Alice in this scheme is trivial. Indeed, when Bob is honest, Δ_i depends on the fact that θ_i fits θ'_i. The probability distribution of Δ_i is then uniform for all $i \in T$ and Alice cannot distinguish I_0, I_1.

Providing that the bit commitment protocol is secure, Yao shown that the above scheme is secure even though Bob can do the coherent attack, i.e. he can attack on multiple quantum states [Yao95]. It was expected that a quantum bit commitment protocol, claimed to be secure [BCJL93], can help to secure Protocol 4.8. However, [May97, LC97] state that quantum bit commitment is impossible.

4.4 MLC No-go Theorems

4.4.1 The Theorems for Pure Two-Party Models

Quantum bit commitment

We can see any bit commitment protocol as a two-phase computation, jointly made by Alice and Bob. After the first phase - commit phase, the computation is interrupted, and then continued in the second phase - opening phase. The computation has the prime input: Alice secret bit to be committed to Bob, and should output one of three values: 0 - if Bob is convinced that Alice's input is $b = 0$; 1 - if Bob is convinced that Alice's input is $b = 1$; and $\perp$ if any cheating user is detected by the other.

As the detection of Bob's cheating would rather be made before the opening phase, we are only interested in the privacy against Bob's (concealment) and the detection of Alice's cheating (binding), once the commit phase has ended, i.e. the computation has been interrupted.

In the classical deterministic computation model, we can easily show that such a scheme is impossible. Indeed, we consider the computation as an evolution in time of *computational configurations* or *images* that consists of variables in Alice and Bob computing

machines, assigned with values. Following a deterministic algorithm, the computation is described by a deterministic sequence of configurations I_{init}, .., I_{final}. At each step i, the configuration of the joint computation is the state of all variables, divided into two parts: Alice's variables and Bob's ones, i.e $I_i = I_i^A \cdot I_i^B$ where "$\cdot$" denotes the concatenation. For the computation of b, the computational configuration sequence following the algorithm will be $\{I_i(b)\}_n$. At the interrupted step int, the configuration is $I_{int}(b) = I_{int}^A(b) \cdot I_{int}^B(b)$. For the protocol being concealing, the partial configurations at Bob side must be identical: $I_{int}^B(0) \equiv I_{int}^B(1)$. Therefore, Alice can freely change the computation by replacing $I_{int}^A(0)$ with $I_{int}^A(1)$ or vise-versa before the opening phase. Thus, the protocol cannot be both concealing and binding.

In the quantum deterministic model, the joint computation is the same as in the above classical model. However, the computation is more physical like: the configuration of the computation at a moment is described by the state of all participating quantum systems at that moment. The transition from one configuration to another successive configuration is made by local unitary transformations at Alice's and Bob's sides and by the communications between them. We would simply consider a pure quantum protocol as a pair of Alice and Bob machines and quantum particles are faithfully brought from sender's machine to receiver's machine in communications.

Similarly to the classical case, according to a deterministic algorithm, Alice and Bob must prepare two quantum systems A and B, characterized by $\mathcal{H} = \mathcal{H}_{A,init} \otimes \mathcal{H}_{B,init}$, initially in some determined pure state $|\psi(b)_{init}\rangle = |\psi(b)\rangle_{A,init} \otimes |0\rangle_{B,init}$. At step i, Alice and Bob realize a joint computation $U_i = U_{A,i} \otimes U_{B,i}$ on $|\psi(b)_{i-1}\rangle$ to get $|\psi(b)_i\rangle$ and communicate to exchange some subsystems, and then, the configuration $|\psi(b)_i\rangle$ is split into two parts according to the new decomposition $\mathcal{H}_{A,i} \otimes \mathcal{H}_{B,i} = \mathcal{H}$. The communication is not restricted to be one-way. We see that $\mathcal{H}$ is invariant, but its decomposition into Alice and Bob's parts varies by communications. The computation is then a determined sequence of configurations $|\Psi(b)_{init}\rangle, .., |\Psi(b)_{final}\rangle$.

At step i, the corresponding configuration $|\Psi(b)_i\rangle$ is split into two partial configurations at Alice and Bob sides:

$$\rho^A(b)_i = tr_{B,i}(|\Psi(b)_i\rangle \langle\Psi(b)_i|),$$
$$\rho^B(b)_i = tr_{A,i}(|\Psi(b)_i\rangle \langle\Psi(b)_i|).$$

If the protocol is unconditionally concealing then Bob has not to be able to distinguish $\rho^B(0)_i$ from $\rho^B(1)_i$ for all $i \leq int$ where int is the interruption step, i.e. $\forall i \leq int, \rho^B(0)_i = \rho^B(1)_i$. Here, it suffices to be only interested in $\rho^B(0)_i = \rho^B(1)_i$ at the interruption step $i = int$. For simplifying, we will use $\mathcal{H}_A \otimes \mathcal{H}_B$ instead of $\mathcal{H}_{A,i} \otimes \mathcal{H}_{B,i}$ to implicitly specify the decomposition at the moment of speaking.

We could expect that Alice cannot replace $\rho^A(0)$ with $\rho^A(1)$ and vice-versa because of the *entanglement* in $|\Psi(b)\rangle$. Unfortunately, following [HJW93], in case $\rho^B(0) = \rho^B(1)$, there exists a unitary transformation U_A acting in $\mathcal{H}_A$ that maps $|\Psi(1)\rangle$ into $|\Psi(0)\rangle$, cf. Theorem 3.3 on page 47. Therefore, Alice can replace the partial configuration by the operators U_A and U_A^{-1}. We would rather say that *quantum entanglement does not help to secure bit commitment.*

More generally, quantum model allows a non-ideal unconditional security, i.e $\rho^B(0) \approx \rho^B(1)$. The security of Alice's bit can be measured by the distinguishability between $\rho^B(0)$

and $\rho^B(1)$, for instance the fidelity of quantum states:

$$F(\rho^B(0), \rho^B(1)) = 1 - \epsilon. \tag{4.2}$$

The extension of Uhlmann's theorem, cf. Theorem 3.5 on page 48, states that there exists a purification $|\Psi'(0)\rangle$ of $\rho^B(1)$ such that

$$|\left\langle \Psi(0) \right| \left. \Psi'(0) \right\rangle| = F(\rho^B(0), \rho^B(1)) = 1 - \epsilon.$$

Recall that, as $|\Psi'(0)\rangle$ and $|\Psi(1)\rangle$ are two purifications of $\rho^B(1)$, there exists a unitary transformation for Alice to switch between $|\Psi'(0)\rangle$ and $|\Psi(1)\rangle$. Therefore, suppose that Alice has began the computation for $b = 1$, she can cheat by transforming $|\Psi(1)\rangle$ into $|\Psi'(0)\rangle$ and declaring $b = 0$. The opening phase will be continued with $|\Psi'(0)_{int+1}\rangle, ... |\Psi'(0)_{final}\rangle$ under unitary transformations. So:

$$|\left\langle \Psi(0)_{final} \right| \left. \Psi'(0)_{final} \right\rangle| = 1 - \epsilon.$$

A measure for Bob accepting Alice announcement is $F(\rho^B(0)_{final}, \rho'^B(0)_{final})$. Following Uhlmann's theorem ([NC04] - theorem 9.4), we have

$$F(\rho(0)^B_{final}, \rho'^B(0)_{final}) \geq 1 - \epsilon. \tag{4.3}$$

Therefore, in a pure deterministic quantum model, we cannot have a bit commitment protocol that is both concealing and binding. Moreover, the more a protocol is concealing, the more it is binding, by the measure of quantum fidelity, cf. Eqs. (4.2), (4.3).

Quantum oblivious transfer

The no-go theorem on bit commitment implies the impossibility of oblivious transfer because we can implement quantum oblivious transfer from bit commitment [Cré94, Yao95]. Though, we revise here Lo's theorem for secure one-sided computations, including oblivious transfer, in a pure deterministic quantum model [Lo97].

Secure one-sided two-party computations is a subclass of secure two-party computations where Alice and Bob want to compute a two-party function $f(i, j)$. Alice holds input i and Bob holds input j. At the end of the computation, Alice has no information about j. Only Bob gets the result $f(i, j)$ and learns no more information about i than what can be learned from his input j and the result $f(i, j)$. For instance, oblivious transfer is a secure one-sided computation of $(1 - c) \times b_0 + c \times b_1$ where Alice inputs b_0, b_1, Bob inputs c.

To compute $f(i, j)$,Alice and Bob run together a unitary U transformation on Alice's input $|i\rangle : i \in \{i_1, .., i_m\}$ joint with Bob's input $|j\rangle : j \in \{j_1, .., j_n\}$. Other known local variables can be omitted without loss of generality. At the end, Bob can learn the result from the output state $|v_{ij}\rangle = U(|i\rangle_A \otimes |j\rangle_B)$. But Alice can entangle her input A with a private quantum ancilla D, i.e. prepares system $D \otimes A$ in the initial state $\frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes |i\rangle_A$.

If Bob inputs j_1 then the initial state for the protocol is

$$\left|u'\right\rangle_{in} = \frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes |i\rangle_A \otimes |j_1\rangle_B , \tag{4.4}$$

and at the end, the output state is

$$|v_{j_1}\rangle = \frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes U(|i\rangle_A \otimes |j_1\rangle_B).$$

Similarly, if Bob inputs j_2 then the output state is

$$|v_{j_2}\rangle = \frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes U(|i\rangle_A \otimes |j_2\rangle_B).$$

For the security on Alice side, the partial configurations must be identical, i.e.

$$tr_B(|v_{j_1}\rangle \langle v_{j_1}|) = tr_B(|v_{j_2}\rangle \langle v_{j_2}|),$$

and then there exists a local unitary transformation U^{j_1,j_2} on Bob local system such that

$$|v_{j_2}\rangle = U^{j_1,j_2} |v_{j_1}\rangle .$$

Therefore, because ${}_D\langle i|\, v_j\rangle = \frac{1}{\sqrt{n}} |v_{ij}\rangle$, the transformation U^{j_1,j_2} is universal for all Alice input i:

$$|v_{ij_2}\rangle = U^{j_1,j_2} |v_{ij_1}\rangle .$$

Bob can enter $|j_1\rangle$, computes $|v_{ij_1}\rangle$ and measures it to learn $f(i, j_1)$. However, to enable Bob to *unambiguously* get the result, $|v_{ij_1}\rangle$ must be an eigenstate of Bob's final measurement and not perturbed by this measurement. Bob can transform it to $|v_{ij_2}\rangle$ by U^{j_1,j_2}, measure it to learn $f(i, j_2)$, and so on. Thus, if the protocol is correct and secure against Alice, Bob can compute $f(i, j)$ for any private input j.

In a non-ideal protocol, Bob could slightly modify $|v_{ij_1}\rangle$ and therefore $|v_{ij_2}\rangle$, when learning j_1, and could learn j_2 with a certain accuracy. The errors are accumulated in each measurement step. The more the protocol is correct, the more Bob can cheat with high accuracy.

4.4.2 Interpretations for the generality

The above canonical theorems for the impossibility of quantum bit commitment and oblivious transfer were made in a deterministic pure two-party quantum model where both parties (i) communicate by sending quantum signal via a quantum channel, and (ii) do all of the computations at the quantum level, following a certain deterministic algorithm.

One may see that this proof is "too simple to be true" for all possible protocols where Alice and Bob (1) do measurement on their quantum systems and pass to classical computation; (2) introduce private secrets; (3) communicate classical information through a macroscopic channel that does permit to transmit quantum signal.

Indeed, the proofs in Mayers' and Lo's - Chau's original papers [May97, LC97] did not interpret in detail the physical operations for the generality of the theorem, clarifying the above three factors. A brutal reduction of the general algorithms to the pure quantum deterministic two-party model could make people doubt its validity. The claim of the

generalization of the theorems caused troubled researchers to try to find a loophole behind it [Yue00, Yue04, Che03] although none of the counter-examples is valid.

Most of attention were paid to classical variables in computations [Yue00, Bub01b, Yue02, Yue04, Che03, Che05, Che06]. Indeed, from a computational viewpoint, the random classical variables are not evident in the deterministic quantum model.

For this, it is stated that probabilistic computations can be implemented by invariant circuits with auxiliary random variables [Gol01], and any classical computation can be realized by equivalent quantum circuits throwing away some parts of outputs, named *superoperators* [BS98], cf. Figure 4.2. The commonly known argument in the main interpretation of no-go theorems is that the computation can be kept at quantum level by not throwing any private quantum system, cf. Figure 4.3. This purifying action on random classical variables is indeed *semi-honest* and cannot be detected. In such a case, the joint computation is deterministic and the canonical proof eliminate the possibility of bit commitment and oblivious transfer protocols, cf. Section 4.4.1.

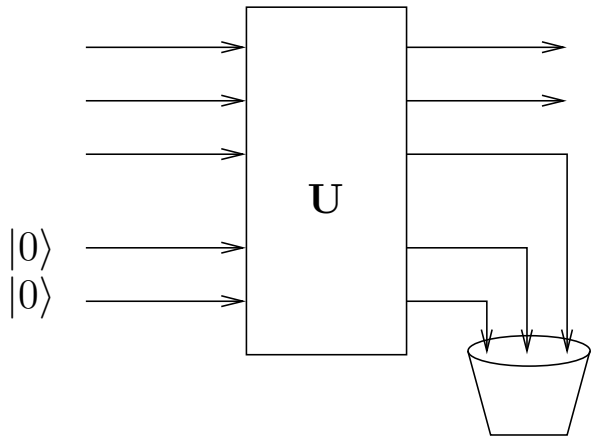

Figure 4.2: Superoperator

The problem of secret variables was addressed in [Yue02, Yue04]. As Alice's cheating transformation is found for the model where Bob does the purification of these random variables, the feeling is that the global state collapses to a secret state depending on Bob's secret classical results, and Alice cannot know the corresponding transformation. This point was partially answered in [Bub01b, Che05, Che06], for ideal and nearly-ideal protocols.

The classical communication is normally omitted with some assumptions on the communication, expressed as "classical communication can be carried out by quantum model, but with some constraints" [LC97]. But what are the constraints? From the physical viewpoint, the classical channel does not appear in this reduced two-party quantum model.

What is the difference between a quantum channel and a classical one? A quantum channel is a medium that we can use to directly transmit a quantum state without disturbing it. Nevertheless a classical channel, for transmitting discrete messages, permits only one from a collection of discrete signal values which can be amplified by many *quantum systems* on

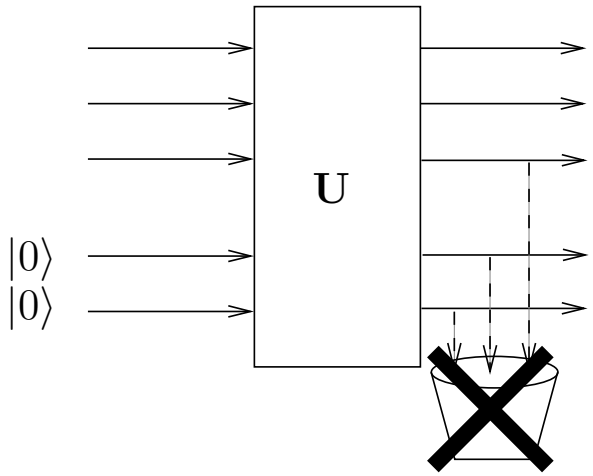

Figure 4.3: Non-throwing superoperator

the channel, for instance a macroscopic electrical wire with tension $+5V$ for 0 and $-5V$ for 1.

Imagine that in the specification of a protocol, at a certain moment, a party S has to measure some quantum state $|\psi\rangle_S$ with an apparatus with n degrees of freedom and communicate this result to the other via a classical channel. This measurement will output $i \in \{1, .., n\}$ with probability $p(i)$ and let the measured system in a state $|\psi_i\rangle_S$. Receiving the classical value i, the receiver R could generate a basis state $|i\rangle_R$ in a n-dimension space for his further computation.

Of course, we can reduce this communication to a pure two-party quantum model where the sender realizes a transformation

$$U(|\psi\rangle_S |0\rangle_R) \rightarrow \sum_{i=1}^{n} \sqrt{p(i)}\, |\psi_i\rangle_S |i\rangle_R$$

and the protocol will go on correctly because the density-matrix description of each system is the same as though a real measurement is done [BCMS97, LC97, Bub01b]. The joint computation remains a unitary evolution of a pure two-pary state, and with such a quantum two-party joint computation, bit commitment is impossible as analyzed in Section 4.4.1.

However, the above reduced model for classical communications does not interpret what really happen in the physical world. It permits to conserve a two-party entanglement that does not exist in the specification of the protocol with classical communication. This two-party entanglement could introduce some extra effects. For instance, it could happen that the receiver used the received message to do a quantum computation and sends back the result, then the sender would learn more information with entanglement attack by the effect of *super-dense coding* [BW92].

Indeed, the classical channel forces the measurements to be done for making classical signals i.e. Alice and Bob have to really measure their quantum states to make classical

messages. In a generic protocol, the communication of classical messages forces destroying the purity of two-party states. The real joint computation with communication by measuring and transmitting classical values via a classical channel is not an evolution of a pure two-party state. In other words, as the action of measurements "can never help a cheater" [GL00], why it does not prevent Alice from cheating?

We can say that a quantum protocol with communication of classical messages can be *correctly* implemented in a pure quantum two-party model. Nevertheless, it is not obvious to emulate the protocol by a purified two-party model for proving the insecurity without a convincing interpretation. One may doubt that the reduced two-party model implements correctly the protocol, not securely, and could be used to prove the possibility [Yao95], not the impossibility of two-party protocols.

This point was only explained in Mayers' version where the measurements for making classical messages were considered [May97]. Following Mayers, Alice and Bob would keep all of the operation at the quantum level, except for making classical messages. Thus, for each classical message γ, the quantum system is projected to a collapsed state corresponding to the classical outcome and is in a known pure two-party state $|\psi_{b,\gamma}\rangle_{AB}$. The trade-off between concealing and binding is separately treated for this state, i.e. the collapsed protocol must be secure:

$$\begin{aligned} F_\gamma &= F\left(\rho_\gamma^B(0), \rho_\gamma^B(1)\right) \\ &= F(tr_A(|\psi_{0,\gamma}\rangle\langle\psi_{0,\gamma}|), tr_A(|\psi_{1,\gamma}\rangle\langle\psi_{1,\gamma}|)) \\ &\geq 1-\epsilon \end{aligned} \tag{4.5}$$

and Alice has a unitary cheating transformation $U_{A,\gamma}$ with possibility of success

$$|\langle\psi_{0,\gamma}|U_{A,\gamma}|\psi_{1,\gamma}\rangle| = F_\gamma \geq 1-\epsilon. \tag{4.6}$$

Chapter 5

Binary Symmetric Multi-Error-Rate Channels

The material of this chapter, based on [Dan07], is concerned with an extended noisy model: the binary symmetric multi-error-rate channel (BSMERC). This channel consists of parallel binary symmetric sub-channels with different error rates.

We see that Crépeau's *et al.*'s [CMW04, Mor05] construction scheme from DMC implements indeed a BSMERC. In their construction, based on this BSMERC, they built a binary symmetric erasure channel by separating the minimal error rate as *good erasure* from the others greater error rates. Then, one can exploit this gap to build an oblivious transfer protocol where Bob can only receive one secret key from Alice, not both, based on error correcting codes and amplification, cf. Section 4.2 on page 52.

However, in some cases, this construction is not efficient as the gap is so tinny. Nevertheless, by considering the general BSMERC, we have the freedom to choose a barrier error rate to make an extended erasure channel which implements oblivious transfer protocol. With such an extension, we can improve the efficiency of the reduction scheme based on the probability distribution of error rates.

We expect also that this general intermediate model is convenient for considering the more general noisy channels, partifularly noisy channels with continuous alphabets.

5.1 Binary Symmetric Multi-Error-Rate Channel

5.1.1 The Model

We extend here the definition of binary symmetric erasure channel to have a binary symmetric multi-error-rate channel (BSMERC) as a binary symmetric channel with different error rates $0 \leq \varphi_1 < ... < \varphi_m \leq 1/2$ with a probability distribution $\sum_j p(\varphi_j) = 1$. For each bit sent on it, the channel chooses to effect a certain error rate φ_j with probability $p(\varphi_j)$. When Bob receives the output bit, he also knows the actual error rate of the channel while Alice does not except with the a priori probability distribution.

We can imagine that the channel consists of m parallel binary symmetric sub-channels

with different error rates. For each input bit, the channel selects a sub-channel j with probability $p(\varphi_j)$ and passes the input via this sub-channel. In another way, the channel is a special discrete memoryless channel with input symbols set $\mathcal{X} = \{0, 1\}$ and output symbols set $\mathcal{Y}$ which can be partitioned into m disjoint binary subsets $\mathcal{Y}_1 \cup ... \cup \mathcal{Y}_m$, $\mathcal{Y}_j = \{y_j^0, y_j^1\}$ where the conditional probability distribution over $\mathcal{X} \times \mathcal{Y}_j$ is $P_{Y/X} \equiv p(\varphi_j) \times P_{Y/X}^{\varphi_j - BSC}$, obtained by the probability distribution of a binary symmetric channel of error rate φ_j (φ_j-BSC) multiplied by $p(\varphi_j)$.

We denote the probabilist set of error rates as $\mathcal{E} = \{p(\varphi_j), \varphi_j\}_{j=1..m}$. We use also $\mathcal{E} = \{\varphi_1, ..., \varphi_m\}$ when the probability distribution $\{p(\varphi_j)\}$ is implicitly agreed. An associated BSMERC to $\mathcal{E}$ can be defined as follows:

Definition 5.1. *$\mathcal{E}$-BSMERC*

1. *Alice sends a bit r.*
2. *Bob receives r' and the outcome of the tossing of a probabilist variable e which takes value in φ_j with probability distribution $\{p(\varphi_j)\}$ which indicates that $Pr(r' \neq r) = \varphi_j$.*

This channel can be faithfully emulated by a quantum coding scheme: the sender encodes a bit by the parity of a sequence of random bits and sends the encoding quantum states of these bits to the receiver, where two values $0, 1$ of a bit are encoded by two nonorthogonal quantum states; the receiver uses the decoding coherent measurement invented by [BMS96] for detecting the parity of the sequence. We will expose this emulation in Chapter 6.

5.1.2 Semi-honest BSMERC from Non-trivial DMC

Indeed, based on a nontrivial DMC, the coding scheme in Protocol 4.3 on page 56 with a pair of input symbols x_1, x_2 satisfying Theorem 4.1 on page 55 can be used to implement a $\mathcal{E}$-BSMERC as follows:

Protocol 5.1. *$P_{Y/X} \to \mathcal{E}$-BSMERC(r)*

1. *Alice encodes $r = 0$ as $x_1.x_2$, $r = 1$ as $x_2.x_1$ and sends them via the DMC.*
2. *Bob receives $y^0.y^1$, sets r' as the best guess of r and the corresponding error rate*

$$e = \frac{P_{Y/X=x_1}(y^{1-r'}) P_{Y/X=x_2}(y^{r'})}{P_{Y/X=x_1}(y^0) P_{Y/X=x_2}(y^1) + P_{Y/X=x_1}(y^1) P_{Y/X=x_2}(y^0)} \in \mathcal{E}.$$

where $\mathcal{E}$ is the set of all possible error rates over all pairs $(y^0, y^1) \in \mathcal{Y} \times \mathcal{Y}$ with input pair x_1, x_2:

$$\mathcal{E} = \left\{ \frac{P_{Y/X=x_1}(y^1) P_{Y/X=x_2}(y^0)}{P_{Y/X=x_1}(y^0) P_{Y/X=x_2}(y^1) + P_{Y/X=x_1}(y^0) P_{Y/X=x_2}(y^1)} \middle| (y^0, y^1) \in \mathcal{Y} \times \mathcal{Y} \right\}$$

then for each $\varphi_j \in \mathcal{E}$

$$\mathcal{Y}\mathcal{Y}_j = \left\{ (y^0, y^1) \in \mathcal{Y} \times \mathcal{Y} \middle| \frac{P_{Y/X=x_1}(y^1) P_{Y/X=x_2}(y^0)}{P_{Y/X=x_1}(y^1) P_{Y/X=x_2}(y^0) + P_{Y/X=x_1}(y^0) P_{Y/X=x_2}(y^1)} = \varphi_j \right\}$$

and

$$p(\varphi_j) = \sum_{(y^0,y^1)\in\mathcal{Y}\mathcal{Y}_j} (P_{Y/X=x_1}(y^0)P_{Y/X=x_2}(y^1) + P_{Y/X=x_1}(y^1)P_{Y/X=x_2}(y^0)).$$

5.1.3 A Characterizing Function of $\mathcal{E}$-BSMERC

Suppose that Alice sends to Bob N random bits via an $\mathcal{E}$-BSMERC, and Bob is free to set a subset of $n = Np$ received bits, $0 \leq p \leq 1$, we are interested in the almost lowest missing information of the bits in Bob's subset, assumed by Law of Large Numbers. For describing this average lowest missing information, we construct a function $\Gamma : [0,1] \to [0,1]$ as:

- if $p \leq p(\varphi_1)$ then Bob almost receives a segment Np bits with error rate e_1 and then $\Gamma(p) = ph(\varphi_1)$;
- if $p(\varphi_1) + p(\varphi_2) \geq p > p(\varphi_1)$ then Bob can almost make the concatenation of a segment of $Np(\varphi_1)$ bits with error rate φ_1 and a segment of $N(p - p(\varphi_1))$ bits with error rate φ_2, then the average entropy is $\Gamma(p) = p(\varphi_1)h(\varphi_1) + (p - p(\varphi_1))h(\varphi_2)$;
- and so on.

An example with an $\mathcal{E}$-BSMERC with 3 error rates is illustrated in Figure 5.1.

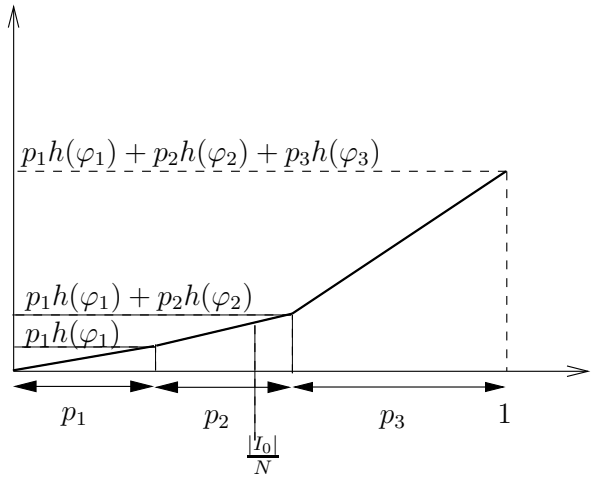

Figure 5.1: Bob's optimal average error rate

5.2 Building Oblivious Transfer from $\mathcal{E}$-BSMERC

We propose an extended BSEC, denoted as $(\mathcal{E}, j_0)$-BSEC, which is defined as a $\mathcal{E}$-BSMERC provided a error rate threshold $\varphi_{j_0} \in \mathcal{E}$ with $1 \leq j_0 < m$. We see that only $(\mathcal{E})$-BSMERC with $\mathcal{E}$ having at least two different error rates, i.e. $m \geq 2$ is interesting for building erasure channels. When $\mathcal{E}$ has only one error rate, the $(\mathcal{E})$-BSMERC becomes in fact a BSC that can be used to produce a BSEC, a BSMERC with two error rates, cf. Protocol 5.1.

Protocol 5.2. *$\mathcal{E}$-BSMERC $\to$ $(\mathcal{E}, j_0)$-BSEC(r)*

1. *Alice sends r via $\mathcal{E}$-BSMERC, and Bob receives r' and $e = \varphi_j$.*
2. *Bob sets $\Delta = 0$ if $e \leq \varphi_{j_0}$, i.e. $j \leq j_0$, and $\Delta = 1$ otherwise.*

This binary symmetric erasure channel has

$$p_g = \sum_{j:\varphi_j \leq \varphi_{j_0}} p(\varphi_j) = \sum_{j \leq j_0} p(\varphi_j). \tag{5.1}$$

Suppose that we have a $\mathcal{E}$-BSMERC with a certain *interesting threshold* $1 \leq j_0 < m$ where m is the cardinality of the error-rate set $\mathcal{E}$, we can inspire from Protocol 4.2 on page 53 for building oblivious transfer.

In our implementations of oblivious transfer, Alice sends $2N$ random bits $r_1, ..., r_{2N}$ to Bob via the $(\mathcal{E}, j_0)$-BSEC with $1 \leq j_0 < m$. Bob should receive $2Np_g$ of them as good bits. Bob then can set two sequences I_0, I_1, each of size $n < 2Np_g$. With I_0, I_1, Bob has two corresponding sequences r'_{I_0}, r'_{I_1} where r'_{I_0} consists of good bits. Then, Alice sends error correcting codes' syndromes $syn(r_{I_0}), syn(r_{I_1})$ for sufficiently correcting all of errors in r'_{I_0}, but not sufficient for correcting all errors in r'_{I_1} for any dishonest setting. We should use error correcting codes with syndrome length

$$|syn(r_{I_0})| = syn(r_{I_1}) = \frac{H_{dis}(r_{I_0}.r_{I_1}/r'_{I_0}.r'_{I_1})/2 + H_{hon}(r_{I_0}/r'_{I_0})}{2} \tag{5.2}$$

where H_{dis} is the missing information for any malicious setting of I_0, I_1 while H_{hon} is the missing information for honest setting. Thus, the missing information gap is crucial for finding efficient error-correcting codes, cf. Theorem 2.3 on page 29:

$$R = |syn(r_{I_0})| - H_{hon}(r_{I_0}/r'_{I_0}) = \frac{H_{dis}(r_{I_0}.r_{I_1}/r'_{I_0}.r'_{I_1}) - 2H_{hon}(r_{I_0}/r'_{I_0})}{4} \tag{5.3}$$

Notice that, with our $(\mathcal{E}, j_0)$-BSEC, r'_{I_0} and r'_{I_1} consist of bits sent via binary symmetric channels with different error rates. For instance, the bits in r'_{I_0} are received with error rates $\varphi_1, ..., \varphi_{j_0}$. We see that, for setting any sequence $r'_{I_0}.r'_{I_1}$ of $2n$-bits length, Bob can in best have almost a segment of $2Np(\varphi_1)$ bits with error rate φ_1, ..., and a last segment of $2N\psi$ (with $\psi \leq p(\varphi_k)$) bits with error rate φ_k such that $2N(p(\varphi_1) + ... + p(\varphi_{k-1}) + \psi) = 2n$, i.e.

$$H_{dis}(r_{I_0}.r_{I_1}/r'_{I_0}.r'_{I_1}) = 2N\Gamma(n/N) \tag{5.4}$$

Besides, for the missing information in honest setting of I_0, we consider two honest settings of I_0 which lead to two different implementation schemes of oblivious transfer as follows.

5.2.1 Scheme 1

In this implementation scheme, we use the exact function for missing information: Bob will create I_0 as the concatenation of segments of positions with error rates $\varphi_j, 1 \leq j \leq j_0$, each of length $2N(p(\varphi_j) - \delta_j)$ with a bias $\delta_j > 0$; and Alice sends the syndromes $syn(r_{I_0}), syn(r_{I_1})$ which are computed by the concatenations of syndromes correcting $2N(p(\varphi_j) - \delta_j)$ uniformly distributed errors with error rate $\varphi_j, 1 \leq j \leq j_0$.

Protocol 5.3. *$(\mathcal{E}, j_0)$-BSEC $\rightarrow$ OT$(b_0, b_1)(c)$*

1. *Alice picks $2N$ random bits r_i, $i = 1, ..., 2N$, and sends to Bob via $(\mathcal{E}, j_0)$-BSEC(r_i). Bob receives r'_i, Δ_i, e_i*

2. *Bob makes two disjoint index sequences I_0, I_1, $|I_0| = |I_1| = n = 2N \sum_{j=1}^{j_0}(p(\varphi_j) - \delta_j)$, such that*

   - *$\Delta_i = 0$ for all $i \in I_0$, i.e. $e_i \leq \varphi_{j_0}$;*
   - *I_0 is the concatenation of segments $1 \leq j \leq j_0$ of $2N(p(\varphi_j) - \delta_j)$ positions the error rate is φ_j.*

   and announces (I_c, I_{1-c}) to Alice.

3. *Alice computes and sends $(s_0 = syn(r_{I_c}), s_1 = syn(r_{I_{1-c}}))$ to Bob. Here, s_0, s_1 are made by the concatenation of codes with error rate φ_j for segment $1 \leq j \leq j_0$ of $2N(p(\varphi_j) - \delta_j)$ bits in r_{I_c}.*

4. *Alice picks a sequence of n random bits m and sends to Bob.*

5. *Alice computes and sends $(\hat{b}_0 = k_0 \oplus b_0, \hat{b}_1 = k_1 \oplus b_1)$ to Bob, with $k_0 = (r_{I_c} \odot m)$, $k_1 = (r_{I_{1-c}} \odot m)$.*

6. *Bob uses s_c to correct errors in r_{I_0}, and computes $b_c = k_c \oplus \hat{b}_c$*

The idea is that Bob almost receives $2Np(\varphi_j)$ bits with error rate φ_j. So, according to the Law of Large Numbers, cf. Theorem 2.1 on page 26, with

$$\forall 1 \leq j \leq j_0, 0 < \delta_j < p(\varphi_j).$$

Bob can almost produce a segment of $2N(p(\varphi_j) - \delta_j)$ indexes where the error rates are φ_j. The missing information to be filled by error correction for this segment is then $2N(p(\varphi_j) - \delta_j)h(\varphi_j)$. So the missing information to be corrected for the sequence r'_{I_0} is

$$H_{hon}(r_{I_0}/r'_{I_0}) = \sum_{j=1}^{j_0} 2N(p(\varphi_j) - \delta_j)h(\varphi_j).$$

Meanwhile, the almost lowest missing information of $r_{I_0}.r_{I_1}$ for all setting of I_0, I_1 is

$$H_{dis}(r_{I_0}.r_{I_1}/r'_{I_0}.r'_{I_1}) = 2N\Gamma\left(2\sum_{j=1}^{j_0}(p(\varphi_j) - \delta_j)\right).$$

Lemma 5.1. *Let error rate set $\mathcal{E} = \{\varphi_1, ..., \varphi_m\}$, for all $1 \leq j < m$ and for all $\lambda > p(\varphi_1) + ... + p(\varphi_j)$ which is decomposed into $\lambda = \lambda_1 + ... + \lambda_j$ such that $\forall 1 \leq i \leq j, \lambda_i \geq p(\varphi_i)$. We have*

$$\sum_{i=1}^{j} \lambda_i p(\varphi_i) < \Gamma(\lambda).$$

Proof. Denote $p = (p(\varphi_1) + ... + p(\varphi_j))$, we have

$$\begin{aligned}\Gamma(\lambda) &\geq \sum_{i=1}^{j} p(\varphi_i)h(\varphi_i) + (\lambda - p)h(\varphi_{j+1}) \\ &= \sum_{i=1}^{j} p(\varphi_i)h(\varphi_i) + \sum_{i=1}^{j} \lambda_i h(\varphi_{i+1}) - \sum_{i=1}^{j} p(\varphi_i)h(\varphi_{i+1}) \\ &= \sum_{i=1}^{j} \lambda_i h(\varphi_{i+1}) - \sum_{i=1}^{j} p(\varphi_i)(h(\varphi_{i+1}) - h(\varphi_i))\end{aligned}$$

and then

$$\Gamma(\lambda) - \sum_{i=1}^{j} \lambda_i p(\varphi_i) \geq \sum_{i=1}^{j} (\lambda_i - p(\varphi_i))(h(\varphi_{i+1}) - h(\varphi_i)).$$

As $\lambda > \sum_{i=1}^{j} p(\lambda_i)$ and $\forall 1 \leq i \leq j, \lambda_i \geq p(\varphi_i)$, there musts exist a certain i such that $\lambda_i > p(\lambda_i)$ and then

$$\Gamma(\lambda) - \sum_{i=1}^{j} \lambda_i p(\varphi_i) > 0.$$

□

Theorem 5.1. *Given a $(\mathcal{E}, j_0)$-BSEC with $1 \leq j_0 < m$ satisfying that there exist $\delta_1, ..., \delta_{j_0}$ such that $\forall 1 \leq j \leq j_0, 0 < \delta_j \leq p(\varphi_j)/2$ and $\sum_{j=1}^{j_0} p(\varphi_j) < \sum_{j=1}^{j_0} 2(p(\varphi_j) - \delta_j) \leq 1$, then Protocol 5.3 implements oblivious transfer with failure probability negligible in N.*

Proof. As $0 < \delta_j \leq p(\varphi_j)$, then Bob can almost honest set up I_0, I_1 where r'_{I_0} is the concatenation of segments, each segment $j = 1..j_0$ has $2N(p(\varphi_j) - \delta_j)$ bits received with error rate φ_j.

Meanwhile, the missing information of $r_{I_0}.r_{I_1}$ for any dishonest setting of I_0, I_1 is:

$$H_{dis}(r_{I_0}.r_{I_1}/r'_{I_0}.r'_{I_1}) = 2N\Gamma\left(2\sum_{j=1}^{j_0}(p(\varphi_j) - \delta_j)\right).$$

As $\forall 1 \leq j \leq j_0, 2(p(\varphi_j) - \delta_j) \geq p(\varphi_j)$, and $\sum_{j=1}^{j_0} 2(p(\varphi_j) - \delta_j) > \sum_{j=1}^{j_0} p(\varphi_j)$, then according to Lemma 5.1:

$$H_{dis}(r_{I_0}.r_{I_1}/r'_{I_0}.r'_{I_1}) > 2N\sum_{j=1}^{j_0} 2(p(\varphi_j) - \delta_j)h(\varphi_j) = 2H_{hon}(r_{I_0}/r'_{I_0}).$$

Therefore, we can propose an error correcting code, with syndrome length calculated by Eq. (5.2), that can correct efficiently $H_{hon}(r_{I_0}/r'_{I_0})$ bits of missing information while there are some remaining bits of missing information of one of r_{I_0}, r_{I_0}. □

Thus, we have to choose $j_0, \delta_1, ..., \delta_{j_0}$ such that

$$\begin{cases} \forall 1 \leq j \leq j_0, 0 < \delta_j \leq p(\varphi_j)/2, \\ \sum_{j=1}^{j_0} p(\varphi_j) < \sum_{j=1}^{j_0} 2(p(\varphi_j) - \delta_j) \leq 1 \end{cases} \tag{5.5}$$

In a convenient way, we can choose $\delta_1 = ... = \delta_{j_0} = \delta$ and the constraints become

$$\begin{cases} 0 < \delta \leq \min_{j=1,...,j_0}\{p(\varphi_j)/2\} \\ \sum_{j=1}^{j_0} p(\varphi_j) < \sum_{j=1}^{j_0} 2(p(\varphi_j) - \delta) \leq 1 \end{cases} \tag{5.6}$$

5.2.2 Scheme 2

In this construction, we consider the received bits in r'_{I_0} as being sent via a BSC with the average error rate

$$\varphi_g = \frac{\sum_{j=1}^{j_0} p(\varphi_j)\varphi_j}{\sum_{j=1}^{j_0} p(\varphi_j)} \tag{5.7}$$

This channel can be emulated as Bob forgets the actual error rate of each received bit in I_0. Then the average missing information to be corrected is $h(\varphi_g)$.

Protocol 5.4. *$(\mathcal{E}, j_0)$-BSEC $\rightarrow$ $OT(b_0, b_1)(c)$*

1. *Alice picks $2N$ random bits r_i, $i = 1, ..., 2N$, and sends to Bob via $\mathcal{E}, \varphi_{j_0}$-BSEC($r_i$). Bob receives r'_i, Δ_i, e_i*
2. *Bob makes two disjoint index sets I_0, I_1, $|I_0| = |I_1| = n = 2N(p_g - \delta)$, such that $\Delta_i = 0$ for all $i \in I_0$, i.e. $e_i \leq \varphi_{j_0}$ and sends (I_c, I_{1-c}) to Alice.*
3. *Alice computes and sends $(s_0 = syn(r_{I_c}), s_1 = syn(r_{I_{1-c}}))$ to Bob. Here, s_0, s_1 made as check codes for error rate $\varphi_g = \frac{\sum_{j=1}^{j_0} p(\varphi_j)\varphi_j}{\sum_{j=1}^{j_0} p(\varphi_j)}$*
4. *Alice picks a sequence of n random bits m and sends to Bob.*
5. *Alice computes and sends $(\hat{b}_0 = k_0 \oplus b_0, \hat{b}_1 = k_1 \oplus b_1)$ to Bob, with $k_0 = (r_{I_c} \odot m)$, $k_1 = (r_{I_{1-c}} \odot m)$.*
6. *Bob uses s_c to correct errors in r_{I_0}, and computes $b_c = k_c \oplus \hat{b}_c$.*

However, by this approach, Bob has lost information when forgetting the error rate of each received bit, as expressed by following inequality, based on the convexity of entropy function:

$$h(\varphi_g) = h\left(\frac{\sum_{j=1}^{j_0} p(\varphi_j)\varphi_j}{\sum_{j=1}^{j_0} p(\varphi_j)}\right) \geq \sum_{j=1}^{j_0} \frac{p(\varphi_j)h(\varphi_j)}{\sum_{j=1}^{j_0} p(\varphi_j)} \tag{5.8}$$

where the right-hand formula is the average missing information when Bob keeps in mind the error rate of each received bit.

Notice that I_0, I_1 are referred to as *sets* in Protocol 5.4 while as *sequences* in Protocol 5.3. The difference is that, if I_0 contains $i_1 < ... < i_n$ then, in Protocol 5.3 Bob sends the sequence $(i_1, ..., i_n)$ while in Protocol 5.3 Bob sends the a permutation sequence $(i_{j_1}, ..., i_{j_n})$ depending on the error rates received at each position.

Obviously, a dishonest Bob should always keep information about error rates, and we cannot apply the average error rate approach to $r'_{I_0}.r'_{I_1}$ for the security. So, for this implementation we should guarantee a positive gap between missing information, cf. Eq. (5.3), as:

$$\Gamma(2(p_g - \delta)) - 2(p_g - \delta)h(\varphi_g) > 0. \tag{5.9}$$

Simply speaking, we can assume that Protocol 5.4 implements an oblivious transfer protocol with failure probability negligible in N with the constraints

$$\begin{cases} 0 < \delta \leq p_g, 2(p_g - \delta) \leq 1, \\ \Gamma(2(p_g - \delta)) - 2(p_g - \delta)h(\varphi_g) > 0 \end{cases} \tag{5.10}$$

5.2.3 Verification of Sender's Honesty

Besides, simply speaking, as the probability distributions of r'_i, Δ_i, e_i are identical over all bits r_i sent by Alice, from the view of Alice I_0 and I_1 cannot be distinguishable, and thus she cannot gain any information about Bob's choice c. So Protocols 5.3, 5.4 are secure against Alice.

However, if we use the binary symmetric erasure channel built from a discrete memoryless channel as in Protocol 5.1, Alice can violate the encoding conventions to change the probability distribution of r'_i, Δ_i, e_i over each r_i in Protocols 5.3, 5.4 and then guess I_0, I_1 to learn c. For preventing this attack we can fortunately verify Alice's honesty by the statistical parameters of the DMC based solely on its output symbols, as in Protocol 4.5 on page 57, because our extensions make only relaxations on the error-rate threshold for the intermediate erasure channels and do not change these parameters.

Protocol 5.5. $P_{Y/X} \to OT(b_0, b_1)(c)$

1. *Alice picks M random bits $b_{1,0}, ..., b_{M,0}$ and sets $b_{l,1} = b_0 \oplus b_1 \oplus b_{l,0}$ for $l = 1, ..., M$.*
2. *Bob picks M random bits $c_1, ..., c_M$.*
3. *For $l = 1, ..., M$, Alice and Bob run a semi-honest OT protocol that use the extended BSEC built from the DMC, cf. Protocol 5.1, Bob gets b'_l with his choice c_l.*
4. *Bob checks the statistics of the channel DMC and aborts if Alice cheats.*
5. *Bob sends $c' = \bigoplus_{l=1}^{M} c_l \oplus c$*
6. *Alice computes $\hat{b}_0 = \bigoplus_{l=1}^{M} b_{l,c'} \oplus b_0$, $\hat{b}_1 = \bigoplus_{l=1}^{M} b_{l,(1-c')} \oplus b_1$ and sends to Bob.*
7. *Bob computes $b_c = \bigoplus_{l=1}^{M} b'_l \oplus \hat{b}_c$.*

5.3 Improvement of Efficiency based on Error-Rate Distribution

We can see that CMW's construction scheme is a special case of Protocols 5.3, 5.4 where $j_0 = 1$. Then, this construction is based on the gap between the minimal error rate and the second least one. However, we see that this choice is not the most efficient for building the oblivious transfer protocol.

For instance, in the example illustrated in Figure 5.1, we have $\varphi_1 \approx \varphi_2$ and $p_1 \approx p_2$. In this case, in the construction of oblivious transfer based in Protocols 4.3 on page 56, 4.2 on page 53, we have to set all $i \in I_0$ with r_i are received with error rate φ_1 and then I_0, I_1 are only made with i where r_i are received with error rate φ_1 or φ_2. Thus, the missing information gap, cf. Eq. (5.3), is very small and causes difficulties in finding effective error-correcting codes to make the oblivious transfer protocol correct and secure.

Nevertheless, we can consider all error rates below a certain value φ_{j_0} as *good* where φ_{j_0} is not necessarily the minimal error rate. With some constraints, cf. Eqs. (5.6), (5.10), we can also build an oblivious transfer protocol from this extended BSEC, cf. Protocols 5.3, 5.4. When we choose $j_0 = 1$, i.e. $\varphi_{j_0} = \varphi_1$, these schemes turn into the above special case.

Moreover, depending on the distribution of error rates corresponding to the output pairs, we would rather choose φ_{j_0} to regroup good pairs with *good error rates* below φ_{j_0}. According to Theorems 2.1 on page 26 and 2.3 on page 29, we should optimize (i) δ for the success of honest setting of I_0 and (ii) the uncertainty gap between the average missing information of r_{I_0} when Bob is honest and of $r_{I_0}.r_{I_1}$ when Bob is dishonest, cf. Eq. (5.3), for an efficient error correcting codes assuming the correctness and the privacy of the protocol.

- For the construction scheme using Protocol 5.3, we would look for a good $j_0 \geq 1$ and a bias δ that optimizes δ and $\Gamma(2(p_g - j_0\delta)) - 2\sum_{j=1}^{j_0}(p(\varphi_j) - \delta)h(\varphi_j)$, satisfying constraints in Eq. (5.6).

- For the construction scheme using Protocol 5.4, the optimization criteria for this construction are then δ and $\Gamma(2(p_g - \delta)) - 2(p_g - \delta)h(\varphi_g)$ with the constraints in Eq. (5.10).

In the above example, cf. Figure 5.1, we would better regroup φ_1, φ_2 as good error rates, and get a better gap between the missing information of r_{I_0}, in honest setting, and of $r_{I_0}.r_{I_1}$, in dishonest setting, for finding out efficient error correcting codes. With such distribution, either Protocol 5.3 or 5.4 can give a better efficiency than the basic construction of [CMW04].

However, the efficiency optimization problem in construction of oblivious transfer is a difficult problem. Our extended schemes can help to improve the efficiency of building oblivious transfer but neither Protocol 5.3 nor 5.4 is an optimal construction.

Imagine that there is a j_0 with $\forall 1 \leq j \leq j_0$, φ_j are very small, $\forall k > j_0$, φ_k are significant, and $p_g = \sum_{j=1}^{j_0} p(\varphi_j) = 1/2 - \epsilon$, then we would think that j_0 is a good choice. Unfortunately, if there exists a $j \leq j_0$ such that $p(\varphi_j) \ll 1$ then $\delta \leq p(\varphi_j)/2$ cannot be optimized. So the construction in Protocol 5.3 is not good in this case. Indeed, the constraints

$0 < \delta \leq \min_{j=1}^{j_0}\{p(\varphi_j)/2\}$ prevent us from seeking for a better threshold. In this case, Protocol 5.4 is better. However, in case of another distribution of error rates where $\forall 1 \leq j \leq j_0$, $p(\varphi_j)$ are so significantly great that we can avoid the constraint on δ but φ_j varies much, then Protocol 5.3 is better because the missing information in r'_{I_0} is computed more accurately and the error correcting codes can be made more efficient.

We should then switch between the two approaches for optimizing both δ and the gap R, cf. Eq. (5.3), depending on the probability distribution of the error rates of the BSMERC.

We can also propose a compromise between two approaches for a better exploitation of the error rate distribution of the BSMERC. We can make partitions over the error rates. Each partition consists of some successive error rates and is considered as in Protocol 5.4 with the average error rate. The global scheme resembles Protocol 5.3, but I_0 is made from concatenation of segments corresponding to the partitions.

Moreover, suppose that we are satisfied with one of the construction, using either Protocol 5.3 or 5.4, the optimization criteria are required to be quantitatively formulated. For instance, in 5.3 construction, we should optimize both δ and $\Gamma(2(p_g - j_0\delta)) - 2\sum_{j=1}^{j_0}(p(\varphi_j) - \delta)h(\varphi_j)$. Therefore, what is the trade-off between these to criteria? This can only determined when we have exact parameters on the efficiency of the error-correcting codes, cf. Theorem 2.3 on page 29.

5.4 Concluding Remarks

In this chapter, we has generalized the construction of oblivious transfer based on a nontrivial discrete memoryless channel by introducing the model of a general binary symmetric multi-error-rate channel, cf. Definition 5.1 and Protocol 5.1. With this extension, we have the freedom to find a threshold for a binary erasure channel which creates a better gap between the equivocation of r_{I_0} to be filled by error-correcting codes and of r_{I_1} to be condensed by privacy amplification.

By this extension, we can enhance the efficiency, i.e. reduce the number of bits sent via the DMC, in comparison with the restricted construction based on the lowest error rate, cf. Protocol 4.3 on page 56. We see that if we can increase both δ and the error rate gap by a factor $\gamma > 1$, then we can reduce N to N/γ to have an oblivious transfer protocol with the same failure probability. However, an efficient construction would depend on the probability distribution of the error rates of the multi-error-rate channel.

Moreover, the construction of oblivious transfer from noisy channels via intermediate BSMERC is more general. We expect that this approach can help us in considering the open question about implementing OT from more general noisy channels such as *continuous alphabet* channels [Mor05]. Intuitively, noisy *continuous alphabet* channels can be used to implement *continuous error-rate set* $\mathcal{E}$-BSMERC. However, it should require further studies for a quantitative analysis of the implementation.

Chapter 6

Quantum Non-Orthogonal Coding

In this chapter, we are studying a quantum nonorthogonal coding scheme using two nonorthogonal quantum pure states. It is known that this coding scheme is comparable to quantum conjugate coding for building QKD protocols [Ben92]. We present an alternative approach to the construction of variants of oblivious transfer, based on the quantum nonorthogonal coding.

If a sender uses this coding to send a classical bit, then there is no quantum measurement apparatus for the receiver to successfully decode the signal. We expose that this coding scheme can be used to emulate the noisy transmission models: BSC, BSEC, BSMERC, mentioned in Chapters 4 and 5. Our constructions are optimal for semi-honest sender model, i.e. in each construction, we explicitly propose an quantum decoding coherent measurement for the receiver to obtain the optimal parameters. We emphasize the advantage of quantum coherent measurements.

Inspired from the previous work, we analyze the construction of an oblivious transfer protocol based on the quantum BSEC with *classically semi-honest sender*. For the security against the receiver, we should consider the optimal coherent attacks, and abandon the usual classical privacy amplification.

Then, it's suggested that we can force the sender to be semi-honest by verifying sender's honesty via statistical tests. A coin flipping based scheme is raised from this idea. However, if the sender is supposed to possess a quantum computer and permitted to keep the quantum entanglement, then the sender can gain information about receiver's secret. In such scenario, we say that the sender is *quantum semi-honest*. Nevertheless, if we have a bit commitment protocol, we can force the sender to be *classically semi-honest sender* and build a secure oblivious transfer protocol.

These results are comparable to what is obtained from the approach based on quantum conjugate coding, cf. Section 4.3 on page 57. However, both of the approaches could not issue a secure quantum oblivious transfer, as prevented by the no-go results of Mayers, Lo & Chau [May97, LC97, Lo97].

6.1 Quantum Non-Orthogonal Coding

We define a β-QNOC as a coding scheme which encodes two possible values of a classical bit (0 or 1) by two quantum nonorthogonal pure states:

$$|\psi_0\rangle, |\psi_1\rangle \quad \text{such that} \quad |\langle\psi_0|\psi_1\rangle| = 1 - \beta. \tag{6.1}$$

For example, we can choose

$$|\psi_0\rangle = \begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}, \quad |\psi_1\rangle = \begin{pmatrix}\cos\alpha\\ -\sin\alpha\end{pmatrix} \tag{6.2}$$

with $\cos 2\alpha = 1 - \beta$. In terms of density matrix, these states are

$$\rho_0 = |\psi_0\rangle\langle\psi_0| = \begin{pmatrix}c^2 & cs\\ cs & s^2\end{pmatrix} \quad \text{and } \rho_1 = |\psi_1\rangle\langle\psi_1| = \begin{pmatrix}c^2 & -cs\\ -cs & s^2\end{pmatrix}$$

where c, s stand for $\cos\alpha, \sin\alpha$ respectively, or shortly

$$\rho_b = \begin{pmatrix}c^2 & \pm cs\\ \pm cs & s^2\end{pmatrix} \tag{6.3}$$

where the plus sign for $b = 0$ and the minus sign for $b = 1$. The parameter β can be seen as a *measure of orthogonality* of the coding scheme: $\beta = 1$ when the two encoding states ρ_1, ρ_2 are orthogonal. Here, we are only interesting in QNOC with $0 < \beta < 1$.

6.2 Optimal Distinguishabilities and Emulated Noisy Models

This is an unusual coding because there is no perfect decoder [NC04]. We can only use some appropriate decoding apparatus, expecting some kinds of distinguishability information [FvdG99].

We expose here some related problems of distinguishability related to this encoding scheme: the distinguishability of the two encoding states themself, and the distinguishability of the parity of a bit sequence encoded by the QNOC. For each optimal quantum measurements for the distinguishabilities, the QNOC can be used to emulate interesting noisy channels.

6.2.1 BSC based on QNOC

The first problem is concerned with the distinguishability of the two encoding non orthogonal pure states.

For example, the distinguishability can be measured by the mutual information between the encoded bit b and the decoding outcomes of a measurement E on the encoding states. This amount of information is bounded by Holevo's inequality [NC04, Yue97]:

$$I(b; E) \leq S(\rho) - \pi_0 S(\rho_0) - \pi_1 S(\rho_1) = S(\rho) \tag{6.4}$$

where $S(.)$ is Von Neumann entropy function, cf. Eq. (3.1) on page 46, $\{\pi_0 = p(b=0), \pi_1 = p(b=1)\}$ is the *a priori* probability distribution of b, and $\rho = \pi_0\rho_0 + \pi_1\rho_1$. It is shown that a projective measurement in basis $\{|+\rangle, |-\rangle\}$ with

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{6.5}$$

is an optimal measurement for the encoding states in Eq. (6.2), gaining the mutual information bound. With this measurement basis, optimizing the mutual information, the QNOC implements a BSC with error rate [BMS96]

$$p_e = \frac{1-2cs}{2} \tag{6.6}$$

where $I(b;E) = 1 - h(p_e)$ for $h(.)$ being binary Shannon entropy function, cf. Eq. (2.2) on page 27.

Protocol 6.1. *QNOC → BSC(r)*

1. *Alice uses the encoding state corresponding to r, cf. Eq.* (6.2) *and sends the qubit to Bob.*
2. *Bob measures the received qubit in basis $\{|+\rangle, |-\rangle\}$, cf. Eq.* (6.5) *and sets $r' = 0$ if the output state is $|+\rangle$, $r' = 1$ if the output state is $|-\rangle$.*

6.2.2 BSEC based on QNOC

On the other hand, the distinguishability can tell us how well one can distinguish the two states ρ_0, ρ_1 in terms of the *conclusive* or *deterministic* information that we can get about the encoded bit from measurement outcomes.

It appears first that we can use the projections $\{\rho_0, I - \rho_0\}$,where I is the identity operator acting on the Hilbert space of $|\psi_0\rangle, |\psi_1\rangle$, to have a conclusive response: when the projection $I - \rho_0$ has acted, then the entry state had to be ρ_1. Thus, the probability of success is equal to $\frac{1}{2}tr((I-\rho_0)\rho_1) = \frac{1}{2}(1 - |\langle\psi_0|\psi_1\rangle|^2)$.

However, deeper studies shown that we would rather couple the system with an ancilla and do a projective measurement in the joint space to gain a better probability of success [Iva87, Die88, Per88, JS95, Bus97]. With an ancilla initialized to be in state $|0\rangle$, the composite system is then in state

$$(c|0\rangle \pm s|1\rangle)|0\rangle = c|00\rangle \pm s|10\rangle$$

where the plus sign for $|\psi_0\rangle$ and minus sign for $|\psi_1\rangle$. We apply the unitary transformation which is a rotation in the subspace spanned by $|00\rangle$ and $|11\rangle$ such that

$$|00\rangle \to \frac{s}{c}|00\rangle + \sqrt{1 - \frac{s^2}{c^2}}|11\rangle.$$

Therefore, the final state is

$$\sqrt{c^2 - s^2}|11\rangle + s(|0\rangle \pm |1\rangle)|0\rangle.$$

If we measure the ancilla system in the basis $\{|0\rangle, |1\rangle\}$ and find it in state $|0\rangle$, then the original state can be conclusively distinguished by the measurement on the original system in the basis $\{|+\rangle, |-\rangle\}$. The probability of a successful inferring is then

$$p_{\max} = 2s^2 = 1 - |\langle\psi_0|\psi_1\rangle| = \beta. \tag{6.7}$$

This measurement is shown to be optimal for a conclusive inferring when $|\psi_0\rangle, |\psi_1\rangle$ are taken with equal probabilities, and the probability in Eq. 6.7 is the optimal probability of success. We see that this decoding scheme implements a BSEC with $p_g = \beta$.

Within the formalism of POVM, we propose a decoding measurement for our β-QNOC with which we can successfully infer the encoded bit with the maximal probability β:

$$\hat{E} = \left\{ \begin{array}{l} \hat{E}_0 = \frac{1}{2-\beta}(I - \rho_1), \\ \hat{E}_1 = \frac{1}{2-\beta}(I - \rho_0), \\ \hat{E}_2 = I - \hat{E}_0 - \hat{E}_1 \end{array} \right\}. \tag{6.8}$$

where the measurement of system in state ρ_1 cannot give $\hat{E} = 0$ and the measurement of system in ρ_0 cannot give $\hat{E} = 1$. In such a way, the encoded bit is conclusively detected when $\hat{E} = 0$ or $\hat{E} = 1$, and we have a binary symmetric erasure channel:

Protocol 6.2. *β-QNOC $\rightarrow$ BSEC(r)*

1. *Alice sends to Bob the state ρ_r encoding r to Bob, using the β-QNOC.*
2. *Bob uses the defined decoding $\hat{E}$, cf. Eq.* (6.8)*, to measure the state. Bob outputs:*
   - $\Delta = 0$ *when* $\hat{E} = 0$ *or* $\hat{E} = 1$*; Bob sets* $r' = \hat{E}$ *and so* $r' = r$*.*
   - $\Delta = 1$ *when* $\hat{E} = 2$*; Bob sets* r' *as random bit.*

Comparing with the BSEC based on quantum conjugate coding, cf. Protocol 4.7 on page 58, we state that

- Protocol 4.7 becomes a noiseless channel if Bob can store the qubit for arbitrarily duration. Nevertheless, Protocol 6.2 cannot be noiseless whatever Bob can do, i.e. there must exist some erasure of information.
- In Protocol 4.7, Alice cannot affect the probability distribution of Δ. Nevertheless, in Protocol 6.2, Alice can affect the probability distribution of Δ by sending a state not belonging to $\{|\psi_0\rangle, |\psi_1\rangle\}$.

6.2.3 The Parity Bit and BSMERC based on QNOC

Suppose that a sender generates a sequence of random bits, encodes each of them by a qubit by the β-QNOC and sends the encoding qubits to a receiver which has to identify the parity of the original bit sequence.

It appears first that the receiver can measure each qubit, optimizing a certain distinguishability information as above, and combining all of the results for determining the

parity bit. However, it is pointed out that the receiver can do better by using a coherent measurement on the whole of the sequence of qubits [BMS96].

The density matrices for the parity bit for a sequence of n qubits is computed recursively as

$$\rho_0^{(n)} = \frac{1}{2}(\rho_0^{(1)} \otimes \rho_0^{(n-1)} + \rho_1^{(1)} \otimes \rho_1^{(n-1)})$$
$$\rho_1^{(n)} = \frac{1}{2}(\rho_0^{(1)} \otimes \rho_1^{(n-1)} + \rho_1^{(1)} \otimes \rho_0^{(n-1)})$$

where the case for a single qubit is exposed in Eq. (6.3):

$$\rho_b^{(1)} = \begin{pmatrix} c^2 & \pm cs \\ \pm cs & s^2 \end{pmatrix}.$$

One defines two auxiliary matrices

$$\rho^{(n)} = \frac{1}{2}(\rho_0^{(n)} + \rho_0^{(n)})$$
$$\Delta^{(n)} = \frac{1}{2}(\rho_0^{(n)} - \rho_0^{(n)}).$$

We have

$$\rho^{(1)} = \begin{pmatrix} c^2 & 0 \\ 0 & s^2 \end{pmatrix}, \quad \Delta^{(1)} = \begin{pmatrix} 0 & cs \\ cs & 0 \end{pmatrix}$$

and $\rho^{(n)}, \Delta^{(n)}$ can be computed recursively as

$$\rho^{(n)} = \rho^{(1)} \otimes \rho^{(n-1)}, \quad \Delta^{(n)} = \Delta^{(1)} \otimes \Delta^{(n-1)}$$

Therefore, $\rho^{(n)}$ is a $2^n \times 2^n$ diagonal matrix in which the diagonal members are 2^n components of the expansion of the tensor $(c^2\ s^2)^{\otimes n}$, for instance $(c^2\ s^2)^{\otimes 2} = (c^4\ c^2s^2\ c^2s^2\ s^4)$, and $\Delta^{(n)}$ is a $2^n \times 2^n$ anti-diagonal matrix in which all of the anti-diagonal members are $c^n s^n$. Thus, by the simple computation

$$\rho_b^{(n)} = \rho^{(n)} \pm \Delta^{(n)},$$

one has the general form of the density matrices for the parity bit

$$\rho_b^{(n)} = \begin{pmatrix} c^{2n} & 0 & 0 & ... & 0 & 0 & \pm c^n s^n \\ 0 & c^{2(n-1)}s^2 & 0 & ... & 0 & \pm c^n s^n & 0 \\ 0 & 0 & c^{2(n-1)}s^2 & ... & \pm c^n s^n & 0 & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & \pm c^n s^n & ... & c^2 s^{2(n-1)} & 0 & 0 \\ 0 & \pm c^n s^n & 0 & ... & 0 & c^2 s^{2(n-1)} & 0 \\ \pm c^n s^n & 0 & 0 & ... & 0 & 0 & s^{2n} \end{pmatrix}.$$

BMS's [BMS96] trick is then a smart re-arranging of rows and columns of the matrix by changing the basis. The new basis vectors are computed from the old ones, $|i\rangle, i \in \{0,1\}^n$, as

$$\left|i'\right\rangle = |i/2\rangle \text{ for even } i, \text{ and } \left|i'\right\rangle = |2^n - (i+1)/2\rangle \text{ for odd } i.$$

We have the parity density matrices in a diagonal form

$$\rho_b^{(n)} = \begin{pmatrix} B_b^{[j=1]} & 0 & ... & 0 \\ 0 & B_b^{[j=2]} & ... & 0 \\ 0 & 0 & ... & 0 \\ 0 & 0 & ... & B_b^{[j=2^{(n-1)}]} \end{pmatrix},$$

where each diagonal member is a 2×2 matrix in the form of

$$B_b^{[j]} = \begin{pmatrix} c^{2(n-k)}s^{2k} & \pm c^n s^n \\ \pm c^n s^n & c^{2k}s^{2(n-k)} \end{pmatrix}.$$

For j from 1 to 2^n: the first block ($j = 1$) has $k = 0$; there are $\binom{n}{1}$ blocks which have $k = 1$; there are $\binom{n}{2}$ blocks which have $k = 2$; etc. This continues until $k = (n-1)/2$ for odd n. For even n, we adjust only $\frac{1}{2}\binom{n}{k}$ blocks of $k = n/2$.

Each of these blocks is of the same form as in Eq. (6.3) and so stands for a QNOC scheme with two pure states

$$|b\rangle^{[k]} = \begin{pmatrix} c'^{[k]} \\ \pm s'^{[k]} \end{pmatrix}, \text{ for } c'^{[k]} = \frac{c^{n-k}s^k}{\sqrt{c^{2(n-k)}s^{2k} + c^{2k}s^{2(n-k)}}}, s'^{[k]} = \frac{c^k s^{n-k}}{\sqrt{c^{2(n-k)}s^{2k} + c^{2k}s^{2(n-k)}}}$$

which encode directly the values of the parity bit b. We will be interested in the optimal mutual information, and each QNOC in a subspace j corresponding to block j is seen as a BSC sub-channel with error rate, cf. Eq. (6.6):

$$p_e^{[k]} = \frac{1 - 2c'^{[k]}s'^{[k]}}{2}.$$

We see that, the encoding scheme randomly selects one of 2^{n-1} orthogonal 2-dimension subspaces $j = 1, ..., 2^{n-1}$ (spanning the basis vectors corresponding to $B_b^{[j]}$) with probability

$$q^{[k]} = tr(B_b^{[j]}) = (c^{2(n-k)}s^{2k} + c^{2k}s^{2(n-k)})$$

and uses two pure states in each subspace to encode to parity bit b whose encoding density matrix is $B_b^{[j]}/tr(B_b^{[j]})$.

The optimal measurement for the mutual information of the parity is then (i) a lossless projective measurement which determines the encoding subspace j and (ii) an optimal measurements for the QNOC using two orthogonal pure states with density matrices $B_b^{[j]}/tr(B_b^{[j]}), b \in \{0, 1\}$, gaining the optimal mutual information $I_2(p_e^{[k]}) = 1 - h(p_e^{[k]})$ with corresponding value k of each sub-channel j.

The optimal mutual information for distinguishing the parity values of the n-bit sequence, with a determined β-QNOC, is then a function that we name by the first letters of its authors Bennett, Mor and Smolin:

$$BMS_\beta(n) = \begin{cases} \sum_{k=0}^{(n-1)/2} \binom{n}{k} q^{[k]} I_2(p_e^{[k]}) & \text{for odd } n \\ \sum_{k=0}^{(n-1)/2} \binom{n}{k} q^{[k]} I_2(p_e^{[k]}) + \frac{1}{2}\binom{n}{n/2} q^{[n/2]} I_2(p_e^{[n/2]}) & \text{for even } n \end{cases}. \tag{6.9}$$

We see that this encoding and decoding schemes implements a binary symmetric multi-error-rate channel, cf. Definition 5.1 on page 68:

Protocol 6.3. *QNOC $\rightarrow$ $\mathcal{E}$-BSMERC(r)*

1. *Alice generates a sequence of n random bits $r_1, ..., r_n$ such that $r_1 \oplus ... \oplus r_n = r$.*
2. *Alice encodes each r_i with a qubit via the QNOC, and sends the qubit sequence to Bob.*
3. *Bob does the above optimal coherent measurement, sets r' as the final guess of r and registers the corresponding error rate $p_e^{[k]}$.*

Thus, $\mathcal{E} = \{p_e^{[k]} | k = 0, ..., \lfloor n/2 \rfloor\}$

The probability of the error rate $p_e^{[k]}$ is then the sum of the usage probabilities of all channels j of the same k:

$$p(p_e^{[k]}) = \begin{cases} \binom{n}{k}(c^{2(n-k)}s^{2k} + c^{2k}s^{2(n-k)}) & \text{for } 1 \leq k \leq (n-1)/2 \\ \frac{1}{2}\binom{n}{k}(c^{2(n-k)}s^{2k} + c^{2k}s^{2(n-k)}) & \text{for } k = n/2 \text{ with even } n \end{cases}. \tag{6.10}$$

6.3 Semi-honest-Sender Oblivious Transfer based on QNOC

6.3.1 Discussion on Protocol Reduction

In the previous section, we have presented how QNOC is used to build several semi-honest-sender noisy channels: BSC, BSEC, BSMERC. We explicitly presented each of constructions of BSC, BSEC and BSMERC from QNOC with an optimal quantum decoding coherent measurement for the optimal parameters. With such channels, we can implement oblivious transfer via the classical reduction scheme, cf. Chapters 4, 5.

The first question is that why did we complicate things, because a BSC is sufficient for implementing all of the others semi-honest channels by the classical reduction schemes, cf. Protocols 4.4 on page 56, 4.3 on page 56.

However, as shown in Sections 6.2.2, 6.2.3, Bob can use coherent quantum measurements with higher capacity beyond classically combining individual measurements. So, in such classical reduction schemes, we should re-examine the possible coherent measurements which would give Bob more advantage.

6.3.2 Construction of OT from Quantum BSEC

We present here the construction of a semi-honest sender oblivious transfer protocol from the quantum BSEC, cf. Protocol 6.2, and highlight the precaution about privacy amplification in the presence of quantum coherent attacks. We use the same reduction scheme as in Protocol 4.2 on page 53 for an oblivious transfer protocol:

Protocol 6.4. *QNOC $\rightarrow \widehat{OT}(b_0, b_1)(c)$*

1. *For i from 1 to N, Alice picks a random bit r_i and sends it to Bob via the BSEC protocol based on β-QNOC; Bob outputs (r'_i, Δ_i).*
2. *Bob randomly builds two disjoint index subsets $I_0, I_1 \subset \{1, ..., N\}$ such that $|I_0| = |I_1| = n$, and $\forall i \in I_0, \Delta_i = 0$.*

3. *Bob sends the ordered pair* (I_c, I_{1-c}) *to Alice, according to his choice* c.

4. *Alice, receiving* (I_c, I_{1-c}), *sends back* $(\hat{b}_0 = b_0 \oplus k_0, \hat{b}_1 = b_1 \oplus k_1)$ *to Bob where* $k_0 = \bigoplus_{i \in I_c} r_i$, $k_1 = \bigoplus_{i \in I_{1-c}} r_i$.

5. *Bob deciphers* $b_c = \hat{b}_c \oplus \bigoplus_{i \in I_0} r'_i$.

We analyze first the correctness P_C and Alice's privacy H_B.

All that Bob receives are a sequence of qubits in a state ρ^B and the ciphertexts of b_0, b_1 with the keys k_0, k_1: $\hat{b}_c = b_c \oplus k_c$, $\hat{b}_{1-c} = b_{1-c} \oplus k_{1-c}$. The equivocations of the plaintexts $H(b_c/\hat{b}_c, \rho^B) = H(k_0/\rho^B)$, $H(b_{1-c}/\hat{b}_{1-c}, \rho^B) = H(k_1/\rho^B)$ depend on Bob's measurements of the qubits ρ^B and his setting of I_0, I_1 [Sha49].

In a classical thinking, we can assume the correctness and Alice's privacy of Protocol 6.4 with classical arguments as for Protocol 4.2.

For the correctness, yes, we can use the same argument as Alice and Bob who are honest can make the scheme as in a classical scenario. P_C is obviously the probability that Bob gets at least n bits in N rounds of BSEC, when Bob is honest.

However, we cannot assume the privacy by these arguments. Following these classical arguments, Bob measures each qubit individually, and combines the results to guess the parity bits of $2n$-bit substrings. Thus, the average error rates in such substrings can help to secure the parity based on the classical privacy amplification. Nevertheless, in the quantum world, dishonest Bob is supposed to use quantum machine with unbounded power. With such a machine Bob can implement quantum algorithms and coherent measurements over the whole of the qubits to gain information. It was shown that in many cases coherent attacks gain much more information than incoherent attack.

For the convenience in our proofs, we adopt a measure of Alice's privacy on Bob side as

$$H_B = H(b_0 \oplus b_1 / Y) \tag{6.11}$$

where Y stands for all intermediate information that Bob can get, and $\oplus$ denotes the exclusive-or operator. Such a measure is reasonable because in many applications built from OT, the security is based on the security of $b_0 \oplus b_1$ [Cré89]. Alice's privacy $H_B = H(b_0 \oplus b_1/\hat{b}_0, \hat{b}_1, \rho^B) = H(k_0 \oplus k_1/\rho^B)$ is the minimal equivocation of the parities of the $2n$-bit substrings of $(r_1, .., r_N)$, given the encoding qubits.

In [BMS96], Bennett *et al.* have proposed the optimal coherent measurement to gain information about the parity of a bit sequence given the non-orthogonal encoding states. However, it's not the same problem as gaining the optimal information about the parity of any of substrings with fixed length. Indeed, we see that when the substrings' length is $2n$ and $2n < N\beta$, we can almost guess the parity of one of them. Figuring out how good a quantum algorithm can guess the parity of any of $2n$-bit substrings of a N-bit string, given the QNOC states, would be complex and out of scope of this thesis.

For convenience, we can simply configure with $2n = N$, and reuse BMS's function, cf. Eq. (6.9), for the optimal accessible information that Bob can get about $k_0 \oplus k_1$ from the

qubits. This amount of information is less than 1 and decreases with N when $\beta < 1$ [BMS96]. Then, $H(k_0 \oplus k_1/\rho^B) = 1 - BMS_\beta(N)$ is greater than 0 and increases with N.

For instance, when we choose $\alpha = 35^o$, thus have $\beta \approx 0.658$, then $BMS_\beta(N)$ is a decreasing function as in Figure 6.1.

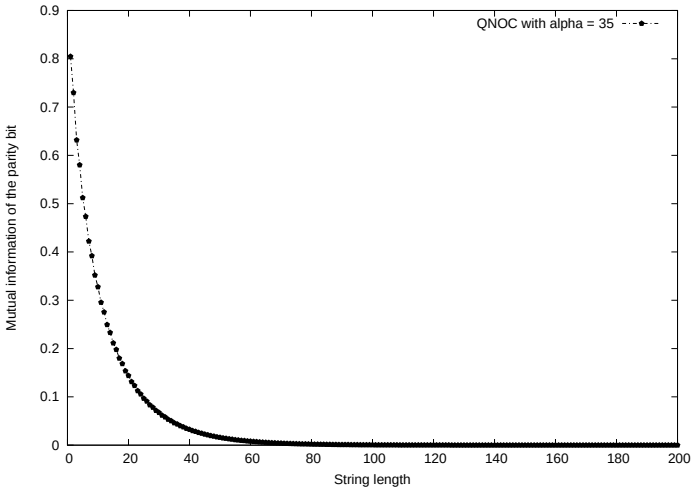

Figure 6.1: Optimal mutual information of the parity bit with 0.658-QNOC

In an asymptotic manner, we have a protocol that is almost both correct and secure against Bob:

Theorem 6.1. *Given any $\epsilon_1, \epsilon_2 > 0$, we can configure Protocol 6.4 with $1/2 < \beta < 1, 2n = N$ and there exists N_0 such that $\forall N \geq N_0$*

$$P_C \geq 1 - \epsilon_1, \quad \textit{and}$$
$$H_B = H(k_0 \oplus k_1/\rho^B) \geq 1 - \epsilon_2.$$

Proof. (Sketch). When Alice and Bob are honest, with $\beta > 1/2$, Bob will receive in average $\beta N > N/2 = n$ good r_i, i.e. with $\Delta_i = 0$. Thus, Bob can set I_0 with no error in r'_{I_0} and successfully decipher b_c. The probability that Bob receives less than $n < \beta N$ good r_i can be negligible in N.

Besides, $H_B = H(k_0 \oplus k_1/\rho^B) = 1 - BMS_\beta(N)$ where $BMS_\beta(N)$ is also negligible in N when $\beta < 1$.

Therefore, we can choose $1/2 < \beta < 1$ for P_C and H_B are both arbitrarily close to 1 with parameter N.

Alice is supposed to be semi-honest, i.e. she respects the QNOC scheme, but wants to record all intermediate information to guess Bob's choice. When Bob is honest, i.e. he respects the decoding scheme, then the probability distribution of Δ_i are identical for all position i, and Alice cannot distinguish I_0, I_1 to gain information about c.

In conclusion, in case Alice is semi-honest, we can configure the protocol with $1/2 < \beta < 1$, $n = N/2$ with even N, Protocol 6.4 implements an oblivious transfer with failure probability arbitrarily small in N. □

6.4 Quantum OT based on Coin Flipping and EPR Attack

We see that Protocol 6.4 does not implement a secure oblivious transfer protocol against Alice who is active. Indeed, Alice can violate the QNOC scheme to control the probability distribution of Δ of the BSEC. Then, simply speaking, the distributions of I_0, I_1 over $\{1, ..., N\}$ are different: a position i with a greater $p(\Delta_i) = 0$ has a greater probability to be put in I_0. Alice can then gain information about c.

For the simple case when the qubit sequence is in state $\rho^B = \bigotimes_{i=1}^{N} \rho^i$, i.e. all ρ^i at position i are not entangled each with the others, then the execution of each i^{th} BSEC round is independent of the others: $p(\Delta_i = 1/\rho^i) = tr(\hat{E}_2 \rho^i)$, where

$$\hat{E}_2 = \begin{pmatrix} \frac{2-2\beta}{2-\beta} & 0 \\ 0 & 0 \end{pmatrix}$$

Thus, Alice cannot definitively force Δ_i to be 1 as $tr(\hat{E}_2 \rho^i) \leq tr(\hat{E}_2) = \frac{2-2\beta}{2-\beta}$. We have

$$\min_{\rho_i} tr(\hat{E}_2 \rho^i) = 0 \quad \text{when } \rho^i = |1\rangle \langle 1| \tag{6.12}$$

$$\max_{\rho_i} tr(\hat{E}_2 \rho^i) = \frac{2-2\beta}{2-\beta} \quad \text{when } \rho^i = |0\rangle \langle 0| \tag{6.13}$$

With such a control of probability distribution of $\Delta_i, i = 1, ..., N$, Alice can guess I_1 as the set with more indices for input $\rho^i = |0\rangle \langle 0|$ and less indices for input $\rho^i = |1\rangle \langle 1|$.

The idea inspired from the implementation of OT from DMC, cf. Protocol 4.5 on page 57, is that Bob should ask Alice to reveal some r_i in Protocol 6.4 to test the encoding. If Alice is supposed to reveal $r_i \in \{0, 1\}$, Bob can measure ρ^i by the projection $\rho_{r_i} = |\psi_{r_i}\rangle \langle \psi_{r_i}|$ to verify. If the qubit is not $|\psi_{r_i}\rangle$, then Alice has a non zero probability of being detected. We should have a protocol as follows:

Protocol 6.5. *$QNOC \rightarrow OT(b_0, b_1)(c)$*

1. *Alice picks M random bits $b_{1,0}, ..., b_{M,0}$ and sets $b_{l,1} = b_0 \oplus b_1 \oplus b_{l,0}$ for $l = 1, ..., M$.*
2. *Bob picks M random bits $c_1, ..., c_M$.*
3. *For $l = 1, ..., M$,*
   - *Alice picks $N + T$ random bits r_i and sends it to Bob via β-QNOC.*
   - *Bob chooses T random indexes j and announces to Alice.*
   - *Alice reveals r_j; Bob measures j^{th} qubit with projection $\left|\psi_{r_j}\right\rangle \left\langle\psi_{r_j}\right|$ and aborts if it fails.*

- *Bob uses the define measurement $\hat{E}$ to complete the BSEC rounds, and Alice and Bob implement $\widehat{OT}(b_{l,0}, b_{l,1})(c_l)$.*

4. *Bob sends $c' = \bigoplus_{l=1}^{M} c_l \oplus c$.*
5. *Alice computes $\hat{b}_0 = \bigoplus_{l=1}^{M} b_{l,c'} \oplus b_0$, $\hat{b}_1 = \bigoplus_{l=1}^{M} b_{l,(1-c')} \oplus b_1$ and sends to Bob.*
6. *Bob computes $b_c = \bigoplus_{l=1}^{M} b'_l \oplus \hat{b}_c$.*

Alice has to cheat all of M $\widehat{OT}$ rounds to learn Bob's choice c. If in each round, dishonest Alice has a non zero probability of being detected, then we can prevent Alice from cheating with large value of M.

With large value of M, we see that the tests assume that each qubit sent by Alice is in state $|\psi_r\rangle$ with a random bit r. This state can be described by $\pi\rho_0 + (1-\pi)\rho_1$. The intuition is that if the i^{th} qubit sent in Protocol 6.4 is in state $\rho^i = \pi\rho_0 + (1-\pi)\rho_1, \pi \in [0,1]$ then $p(\Delta_i = 0) = \beta$. We would deduce from the classical case that if the probability distributions of all Δ_i are identical, then Alice cannot discover c.

Nevertheless, Bob can use his advantage to cheat in each $\widehat{OT}$ round: he measures all of the $N+T$ qubits and ask Alice to reveal r_j with which the result is bad while using good result to set I_0, I_1. Bob can cheat one of M $\widehat{OT}$ rounds to flaw the protocol. However, we would expect a good configuration of M and N to make Protocol 6.5 highly secure against both Alice and Bob as in [Mor05].

Based on the same idea, we would conclude that, if Alice and Bob have access to a coin flipping protocol, e.g. a black box that generates pairs of random bits, then Bob's advantage is removed. We would imagine an oblivious transfer protocol based on coin flipping as follows:

Protocol 6.6. *CF and QNOC $\rightarrow$ OT$(b_0, b_1)(c)$*

1. *For i from 1 to $(M+1)N$, Alice picks a random bit r_i and sends to Bob a quantum states encoding r_i with β-QNOC scheme.*
2. *Alice and Bob use coin flipping to generate N random $\log(M+1)N$-bit numbers to select $U \subset \{1, ..., (M+1)N\}$ with $|U| = N$.*
3. *For $i \in T = \{1, .., (M+1)N\} \setminus U$, Alice unveils r_i to Bob; Bob verifies r_i by measuring the i^{th} qubit ρ^i with the projection $|\psi_{r_i}\rangle\langle\psi_{r_i}|$ and abort if it fails.*
4. *Alice and Bob continue with Protocol 6.4 on N remaining qubits indexed in U.*

Unfortunately, this classical reasoning is true only if the state $\pi\rho_0 + (1-\pi)\rho_1$ is prepared by a statistic ensemble consisting of $|\psi_0\rangle$ with probability π and $|\psi_1\rangle$ with probability $1-\pi$. In the scope of quantum mechanics, this statistical ensemble can be prepared as the state of a subsystem entangled with another system.

In general case, Alice prepares a bipartite state ρ^{AB}, and sends to Bob N qubits in the state

$$\rho^B = tr_A(\rho^{AB}).$$

For instance, Alice can violate the encoding convention by preparing each qubit as half B of a pair in state

$$\sqrt{\pi}\,|0\rangle_A \otimes |\psi_0\rangle_B + \sqrt{1-\pi}\,|1\rangle_A \otimes |\psi_1\rangle_B$$

and sends the qubit B to Bob. This preparation is indeed *quantum semi-honest* because the density matrix of the qubit B is the same as when Alice is honest. When Bob measures the qubit B with the defined $\hat{E}$ for implementing Protocol 6.2, the probability distribution of Δ does not change, $p(\Delta/\rho^B = 0) = \beta$. However, Alice can measure the system A with some apparatus E_A to gain some mutual information $I(\Delta; E_A)$ about Δ based on the correlation produced by quantum entanglement. Alice can then use $I(\Delta_i; E_A)$ about Δ_i in each i^{th} round to guess the difference between I_0 and I_1.

We expose here an example of such EPR attacks on Protocol 6.6. By similarity, this attack also flaws Protocol 6.5. Assume that

$$|\psi_0\rangle = \sqrt{1-\frac{\beta}{2}}\,|0\rangle + \sqrt{\frac{\beta}{2}}\,|1\rangle\,, \quad |\psi_1\rangle = \sqrt{1-\frac{\beta}{2}}\,|0\rangle - \sqrt{\frac{\beta}{2}}\,|1\rangle\,.$$

then

$$\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1 = \begin{pmatrix} 1-\frac{\beta}{2} & 0 \\ 0 & \frac{\beta}{2} \end{pmatrix} = (1-\frac{\beta}{2})\,|0\rangle\langle 0| + \frac{\beta}{2}\,|1\rangle\langle 1|$$

This matrix can be prepared as an ensemble of $|0\rangle$ with probability $(1-\frac{\beta}{2})$ and $|1\rangle$ with probability $\frac{\beta}{2}$. We see that these states maximally violate the β-QNOC and have the best distinguishability of the probability distributions of Δ, cf. Eq. (6.12), (6.13).

Therefore, a dishonest Alice can make a bipartite state

$$\left|\phi'\right\rangle = \sqrt{1-\frac{\beta}{2}}\,|0\rangle_A\,|0\rangle_B + \sqrt{\frac{\beta}{2}}\,|1\rangle_A\,|1\rangle_B$$

and sends qubit B to Bob. Observe that the density matrix of Bob's part is the same as the density matrix of Bob's part of $|\phi\rangle = (|0\rangle_A\,|\psi_0\rangle_B + |1\rangle_A\,|\psi_1\rangle_B)/\sqrt{2}$, and there exists a unitary transformation U_A on Alice side that transforms $|\phi'\rangle$ to $|\phi\rangle$: $(U_A \otimes I_B)\,|\phi'\rangle = |\phi\rangle$. We have

$$\begin{aligned}
\left|\phi'\right\rangle &= \sqrt{1-\frac{\beta}{2}}\,|0\rangle_A\,|0\rangle_B + \sqrt{\frac{\beta}{2}}\,|1\rangle_A\,|1\rangle_B \\
&= \sqrt{1-\frac{\beta}{2}}\,\frac{(|+\rangle_A + |-\rangle_A)}{\sqrt{2}}\,|0\rangle_B + \sqrt{\frac{\beta}{2}}\,\frac{(|+\rangle_A - |-\rangle_A)}{\sqrt{2}}\,|1\rangle_B \\
&= \frac{1}{\sqrt{2}}\,|+\rangle_A \otimes \left(\sqrt{1-\frac{\beta}{2}}\,|0\rangle_B + \sqrt{\frac{\beta}{2}}\,|1\rangle_B\right) + \frac{1}{\sqrt{2}}\,|+\rangle_A \otimes \left(\sqrt{1-\frac{\beta}{2}}\,|0\rangle_B - \sqrt{\frac{\beta}{2}}\,|1\rangle_B\right) \\
&= \frac{1}{\sqrt{2}}(|+\rangle_A \otimes |\psi_0\rangle_B + |-\rangle_B \otimes |\psi_1\rangle_B)
\end{aligned}$$

and thus U_A is indeed the Hadamard gate

$$U_A = H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Therefore:

- If the state $|\phi'\rangle$ is selected to be tested, Alice can apply U_A on her side to have $|\phi\rangle$ and measures the system A in the basis $\{|0\rangle_A, |1\rangle_A\}$. This is equivalent for Alice to measure in basis $\{|+\rangle_A, |-\rangle_A\}$. Alice reveals $r = 0$ if the output is $|0\rangle_A$ leaving Bob's part in state $|\psi_0\rangle_B$, $r = 1$ if the output is $|1\rangle_A$ leaving Bob's part in state $|\psi_1\rangle_B$. Alice can then successfully pass the test.

- If the state $|\phi'\rangle$ is used for OT protocol, Alice measures the system A in the basis $\{|0\rangle_A, |1\rangle_A\}$. If Alice outputs $|0\rangle_A$, Bob is left with the state $|0\rangle_B$ that has a higher probability of giving $\Delta = 1$; if Alice outputs $|1\rangle_A$, Bob is left with the state $|1\rangle_B$ that has a lower probability of giving $\Delta = 1$. We remark that Alice's and Bob's measurements commute in the sense that, if Alice measures after Bob does, Alice gain the same informations, i.e. Bob has received $\Delta = 1$ with a higher probability if Alice outputs $|0\rangle_A$ and Bob has received $\Delta = 1$ with a lower probability if Alice outputs $|1\rangle_A$.

With such an advantageous information about probability distribution of $\Delta_i, i \in U$, given I_c, I_{1-c}, Alice can guess I_1 as the set with more indices for output $|0\rangle_A$ and less indices for output $|1\rangle_A$. Therefore, the tests cannot help us to prevent Alice from cheating, and the above quantum oblivious transfer protocols, even though based on coin flipping, are flawed by EPR attacks.

6.5 Quantum OT based on Bit Commitment

We see that Protocol 6.4 is secure against Alice only if Alice is supposed to respect the encoding convention in the β-QNOC scheme. We can force Alice to do this with help of a bit commitment protocol. Recall that coin flipping can be built from bit commitment [CK88].

Protocol 6.7. *BC and QNOC* $\rightarrow$ *OT*$(b_0, b_1)(c)$

1. *Alice picks* $(M+1)N$ *random bits* r_i *and commits all of* r_i *to Bob via BC protocol.*

2. *Alice sends to Bob quantum states encoding* r_i *with* β*-QNOC scheme for all* $i = 1, ..., (M+1)N$.

3. *Alice and Bob use coin flipping, which can be built from BC, to generate* N *random* $\log((M+1)N)$*-bit numbers to select* $U \subset \{1, ..., (M+1)N\}$ *with* $|U| = N$.

4. *For* $i \in T = \{1, .., (M+1)N\} \setminus U$,

   - *Alice unveils* r_i *to Bob.*
   - *Bob verifies* r_i *in the commitment and aborts if it fails.*
   - *Bob measures the* i^{th} *qubit with the projection* $|\psi_{r_i}\rangle \langle\psi_{r_i}|$ *and abort if it fails.*

5. *Alice and Bob continue with Protocol 6.4 on* N *remaining qubits indexed in* U.

The main difference between the test with a commitment of r and the one without a commitment as in Protocols 6.5, 6.6 is that a committed bit r, with the projection $|\psi_r\rangle \langle\psi_r|$, determines only the pure state $|\psi_r\rangle$ while a random bit r with the projection $|\psi_r\rangle \langle\psi_r|$ is a

mixed state described by $\pi |\psi_0\rangle \langle\psi_0| + (1-\pi) |\psi_1\rangle \langle\psi_1|$. Then, the former case does not permit Alice to send the encoding qubit different from the conventional pure state $|\psi_r\rangle$ while the later permits a violation of β-QNOC by part of a bipartite entangled state. In other words, the commitment of r forces Alice to be *classically semi-honest*.

Therefore, in Protocol 6.7, if dishonest Alice violates the β-QNOC convention for some rounds of BSEC in U to have some chance to distinguish $I_0, I_1 \subset U$, then she will be detected with large value of M. If Alice pass the tests then Alice musts almost respect the encoding convention. Thus following Theorem 6.1, she gains little information about c.

Could EPR attacks help Alice to cheat in a general way: Alice prepares ρ^{AB} and sends the qubit sequence in state $\rho^B = tr_A(\rho^{AB})$ to Bob; after the selection of U, Alice operates on ρ^A in such a way that Bob's part in U violates the β-QNOC and helps Alice to guess c, cf. Sections 6.6 and 6.4, while Bob's part not in U, named $\overline{U}$, passes the tests? We see that with a large value of M, almost qubits in $\overline{U}$ must respect the β-QNOC. So, there may exist $U' \subset \overline{U}, |U'| = |U|$ such that the qubit sequence in U' respects the QNOC, i.e. is in state $\bigotimes_{i\in U'} |\psi_{r_i}\rangle \langle\psi_{r_i}|$ and so

$$\rho^B = \left(\bigotimes_{i\in U'} |\psi_{r_i}\rangle \langle\psi_{r_i}| \right) \otimes \rho^{\overline{U'}}$$

As U' and U are equivalent under the random selection, Alice's operation would also work with U' as U. However, for any of Alice's local transformations, ρ^B remains the same, i.e. the qubit sequence in U' is in state $\bigotimes_{i\in U'} |\psi_{r_i}\rangle \langle\psi_{r_i}|$ that respects the β-QNOC and does not help Alice.

Theorem 6.2. *Given $\epsilon_1, \epsilon_2, \epsilon_3 > 0$, we can configure Protocol 6.7 with $1 > \beta > 1/2$, $N/n = 2$ and there exists N_0 such that $\forall N \geq N_0$*

$$P_C \geq 1 - \epsilon_1, \quad \textit{and} \quad H_B \geq 1 - \epsilon_2,$$

and there exists M_0 depending on N such that $\forall M \geq M_0$

$$H_A \geq 1 - \epsilon_3$$

Proof. (Sketch) Following Theorem 6.1 we could configure Protocol 6.4 and choose first a large value of N_0 to have an oblivious transfer protocol strongly correct and secure against Bob:

$$P_C \geq 1 - \epsilon_1, \quad \text{and} \quad H_B \geq 1 - \epsilon_2$$

Then, we choose M large enough to assume that at the conclusion of Protocol 6.7, Alice has to almost respect the β-QNOC and gains an amount of information about c below ϵ_3. □

6.6 Building Weak Oblivious Transfer

We will show that Protocol 6.4 satisfies Definition 4.1 on page 52 with $P_C > 0, H_B > 0, H_A > 0$.

The correctness parameter P_C is considered, given that Alice and Bob are both honest. We see that $P_C = \sum_{N\geq a\geq n} \binom{N}{a} \beta^a (1-\beta)^{N-a}$. Thus $P_C > 0$ when $0 < \beta < 1$. Besides, Alice's

privacy H_B is $1 - BMS_\beta(N)$ when we choose $n = N/2$ for even N. And then, $H_B > 0$ when $\beta < 1$.

We consider now the security on Alice side, i.e. Bob-privacy when Bob is honest. We denote D, the probability distribution of N BSEC rounds $e = (\Delta_1, ..., \Delta_N) \in \{0,1\}^N$, known to Alice when Bob is honest. In fact, Alice can control the probability distribution D of execution of BSEC rounds $e = (\Delta_1, .., \Delta_N)$ by sending a sequence of qubits in any state.

$$H_A = \min\{H(c/D) : \text{for all } D \text{ that Alice can generate by sending the quantum sequence}\}$$

Given a distribution D, Alice has an equivocation of Bob's choice as the average entropy

$$\mathbf{H_A} = H(c/D) = \sum_{W \in \mathcal{W}} p(W/D) H(c/W, D), \tag{6.14}$$

for $\mathcal{W}$ being the set of all ordered pairs of disjoint subsets of n indexes, i.e.

$$\mathcal{W} = \{W = (W_0, W_1) : W_0 \cap W_1 = \emptyset, |W_0| = |W_1| = n\},$$

and $H(c/W, D) = h(p(c = 0/W, D))$ being the conditional entropy of c when Alice receives $W \in \mathcal{W}$. Thus:

$$\begin{aligned}
p(c = 0/W, D) &= \frac{p(W/c = 0, D) p(c = 0/D)}{p(W/D)} \\
&= \frac{p(W_0 = I_0, W_1 = I_1/D)}{2p(W/D)} \\
&= \frac{\sum_e p_D(e) p(W_0 = I_0, W_1 = I_1/e)}{2 \sum_e p_D(e) p(W/e)}, \\
p(c = 1/W, D) &= \frac{p(W/c = 1, D) p(c = 1/D)}{p(W/D)} \\
&= \frac{p(W_1 = I_0, W_0 = I_1/D)}{2p(W/D)} \\
&= \frac{\sum_e p_D(e) p(W_1 = I_0, W_0 = I_1/e)}{2 \sum_e p_D(e) p(W/e)}
\end{aligned}$$

where $p(I/e)$ is the probability that Bob returns W to Alice, knowing an occurrence e of the executions with the probability $p_D(e)$ controlled by Alice.

The probability that Bob returns $W = (W_0, W_1)$, given the execution e, is computed by the formula

$$p(W/e) = \sum_{k=0}^{1} p(W_k = I_0, W_{1-k} = I_1/e).$$

We suppose that honest Bob, knowing an execution $e = (\Delta_1, .., \Delta_N)$, randomly selects I_c as any subset of L indexes from $Zero(e) = \{i \in \{1, .., N\} | \Delta_i = 0\}$, and fills I_{1-c} with the remaining indexes in $Zero(e)$, then with indexes randomly selected from $One(e) = \{1, ..., N\} \setminus Zero(e)$.

For $W = (W_0, W_1) \in \mathcal{W}$, we have

$$p(W_0 = I_0, W_1 = I_1/e) = \begin{cases} \binom{|Zero(e)|}{2n}^{-1} & \text{if } W \subset Zero(e) \\ \binom{|Zero(e)|}{n}^{-1} \binom{|One(e)|}{2n-|Zero(e)|}^{-1} & \text{if } W_0 \subset Zero(e) \wedge Zero(e) \subset W \\ 0 & \text{otherwise.} \end{cases}$$

We denote $\mathcal{E}_W = \{e : p(W_0 = I_0, W_1 = I_1/e) > 0\}$ i.e. $W \in Zero(e)$ or $W_0 \subset Zero(e) \wedge Zero(e) \subset W$. For $0 \leq a \leq N$, we use e^a to denote any occurrence of e such that $Zero(e) = a$. The cardinality of $\mathcal{E}_W^a = \{e^a \in \mathcal{E}_W\}$ is then

$$|\mathcal{E}_W^a| = \begin{cases} \binom{N-2a}{a-2n} & \text{if } a \geq 2n \\ 1 & \text{if } n \leq a < 2n \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$\begin{aligned} p(W_0 = I_0, W_1 = I_1/D) &= \sum_{N \geq a \geq 0} \sum_{e^a} p(e^a/D) p(W_0 = I_0, W_1 = I_1/e^a) \\ &= \sum_{N \geq a \geq 0} \sum_{e^a \in \mathcal{E}_W^a} p(e^a/D) p(W_0 = I_0, W_1 = I_1/e^a) \\ &= \sum_{N \geq a \geq 2n} \sum_{e^a \in \mathcal{E}_W^a} p(e^a/D) p(W_0 = I_0, W_1 = I_1/e^a) \\ &\quad + \sum_{2n > a \geq n} \sum_{e^a \in \mathcal{E}_W^a} p(e^a/D) p(W_0 = I_0, W_1 = I_1/e^a) \end{aligned}$$

We see that, only a i^{th} qubit with *a priori* probability known by Alice $p(\Delta_i = 1) = 1$ can give Alice the conclusive information about c when i is put into I_1 by Bob.

However, when Bob uses the decoding measurement $\hat{E}$ for the β-QNOC with $\beta > 0$, $p(\Delta_i = 1/\rho^i) \leq \frac{2-2\beta}{2-\beta} < 1$ for all quantum states ρ^i sent to Bob, cf. Eq. 6.13. Therefore, for all cheating qubits sent to Bob, Alice has nonzero uncertainty about c, i.e. $H_A > 0$.

In brief, as analyzed above, Protocol 6.4 satisfies Definition 4.1 when $0 < \beta < 1$. The parameters N, n and β can be calibrated to have some degree of weak correctness and weak security on both sides. We enter then in a two-party game where the more advantage we give to a party, the more this party can control the game and cheat.

We omit a quantitative analysis for the configuration of our WOT because of the complexity on Alice side. Intuitively, the smaller β is, the larger Alice-privacy H_B is, but the smaller Bob's privacy H_A is because Alice has larger gap in the probability distribution of $\Delta_i : 0 \leq p(\Delta_i = 1) \leq \frac{2-2\beta}{2-\beta}$. Besides, the smaller N is, the smaller Alice-privacy H_B is, but the larger Bob-privacy H_A is because it is harder for Alice to distinguish I_0 and I_1.

We expect that if the protocol is configured to be correct and secure on Bob side, Alice will be able to generate a distribution D to guess c with a high accuracy. Indeed, a quantum oblivious transfer that is correct and secure on both sides is eliminated by the no-go theorems ([May97, LC97, Lo97]) that we will expose in the next chapter.

Chapter 7

No-go Theorems: Reinterpretation and Extension

The material of this chapter is concerned with the general model of quantum two-party protocols. Such protocols should consist of communication of quantum information via a quantum channel and classical information via a macroscopic channel. With the presence of such macroscopic channel, a quantum protocol is no more a purely quantum two-party model consisting of users' quantum machines. The measurements for making classical signals transmitted via this channel would create entanglements between users' quantum systems with a third party system, uncontrollable by the users and thrown to the environment. The macroscopic channel is as a public measurement apparatus which is trusted by both Alice and Bob.

With this three-party model including an environment party coupled with the classical channel, we present a faithful interpretation of general quantum protocols for building bit commitment and oblivious transfer protocols. With the purified model, we show that the no-go theorems are valid for both ideal and non-ideal primitives.

Based on this interpretation for general two-party protocols, showing certain features of the models penalized by the theorem, we extend the no-go theorem for some particular trusted two-party oracle based models which do not hide information from the views of Alice and Bob. A no-go result on coin-flipping based bit commitment protocols similar to Kent's one [Ken99] can be easily obtained from these extensions.

A corollary from these extensions is that a quantum two-party oracle for implementing unconditionally secure bit commitment and oblivious transfer must involve an erasure of information from the views of Alice and Bob. This remark suggests us to discuss the no-go theorems from a thermodynamical point of view, due to Landauer's principle [Lan61].

7.1 Reinterpretation for No-go Theorems

A major objection to MLC no-go theorem is that it is "too simple to be true" for all possible protocols where Alice and Bob

1. do measurement on their quantum systems and pass to classical computation;

2. introduce private secrets;

3. communicate classical information through a macroscopic channel that does not permit to transmit quantum signal.

Most of attention were paid to classical variables in computations [Yue00, Bub01b, Yue04, Che03, Che06]. And these were successfully explained in these supplement works. The problem of secret variables, addressed in [Yue02, Yue04], was also treated for ideal and nearly ideal protocols by some related results in [Bub01b, Che06].

The classical communication is normally omitted with some assumptions on the communication, expressed as "classical communication can be carried out by quantum model, but with some constraints" [LC97]. But what are the constraints? From a physical viewpoint, the classical channel does not appear in this reduced two-party quantum model.

What is the difference between a quantum channel and a classical one? A quantum channel is a medium that we can use to directly transmit a quantum state without disturbing it. Nevertheless a classical channel, for transmitting discrete messages, permits only one from a collection of discrete signal values which can be amplified by many *quantum systems* on the channel, for instance a macroscopic electrical wire with tension $+5V$ for 0 and $-5V$ for 1.

Imagine that in the specification of a protocol, at a certain moment, a party S has to measure some quantum state $|\psi\rangle_S$ with an apparatus with n degrees of freedom and communicate this result to the other via a classical channel. This measurement will output $i \in \{1, .., n\}$ with probability $p(i)$ and let the measured system in a state $|\psi_i\rangle_S$. Receiving the classical value i, the receiver R could generate a basis state $|i\rangle_R$ in a n-dimension space for his further computation.

Of course, we can reduce this communication to a pure two-party quantum model where the sender realizes a transformation

$$U(|\psi\rangle_S \otimes |0\rangle_R) \rightarrow \sum_{i=1}^{n} \sqrt{p(i)}\, |\psi_i\rangle_S \otimes |i\rangle_R$$

and the protocol will go on correctly because the density-matrix description of each system is the same as though a real measurement is done [LC97, Bub01b]. The joint computation remains an unitary evolution of a pure two-party state, and with such a quantum two-party joint computation, bit commitment is impossible as analyzed in Section 4.4.1.

However, the above reduced model for classical communications does not interpret what really happen in the physical world. It permit to conserve a two-party entanglement that does not exist in the specification of the protocol with classical communication. This two-party entanglement could introduce some extra effects. For instance, it could happen that if the receiver uses the received message to do a quantum computation and sends back the result, the sender could learn more information with entanglement attack by the effect of *super-dense coding* [BW92].

We can say that a quantum protocol with communication of classical messages can be *correctly* implemented in a pure quantum two-party model. Nevertheless, it is not obvious to emulate the protocol by a purified two-party model for proving the insecurity without a

convincing interpretation. We have right to doubt that the reduced two-party model may implement correctly the protocol, not securely. The pure quantum two-party model could be used to prove the possibility [Yao95], not the impossibility.

Indeed, the classical channel forces the measurements to be done for making classical signals i.e. Alice and Bob have to really measure their quantum states to make classical messages. And in a generic protocol, the communication of classical messages forces destroying the purity of two-party states. The real joint computation with communication by measuring and transmitting classical values via a classical channel is not an evolution of a pure two-party state. In other words, as the action of measurements "can never help a cheater", why it does not prevent Alice from cheating?

This point was only explained in Mayers' version where the measurements for making classical messages were considered [May97]. Following Mayers, Alice and Bob would keep all of the operation at the quantum level, except for making classical messages. Thus, for each classical message γ, the quantum system collapsed with the corresponding classical outcome is in a known pure two-party state $|\psi_{b,\gamma}\rangle_{AB}$, and the trade-off between concealing and binding is separately treated for this state, i.e. the collapsed protocol must be secure:

$$\begin{aligned} F_\gamma &= F\left(\rho_\gamma^B(0), \rho_\gamma^B(1)\right) \\ &= F(tr_A(|\psi_{0,\gamma}\rangle\langle\psi_{0,\gamma}|), tr_A(|\psi_{1,\gamma}\rangle\langle\psi_{1,\gamma}|)) \\ &\geq 1-\epsilon \end{aligned} \tag{7.1}$$

and Alice has a unitary cheating transformation $U_{A,\gamma}$ with possibility of success

$$|\langle\psi_{0,\gamma}| U_{A,\gamma} |\psi_{1,\gamma}\rangle| = F_\gamma \geq 1-\epsilon. \tag{7.2}$$

However, a protocol that is secure against Bob is not necessarily secure for all possible collapsed protocols corresponding to all possible classical exchanged messages, cf. Eqs. (7.1) and (7.2), but on average. For example, F_γ could be small for some γ but the occurring probability of γ is small. Moreover, it can happen that the occurring probabilities of γ for the commitment of 0 and 1 are different, i.e. $p_0(\gamma) \neq p_1(\gamma)$. Could we relax more the measures of average concealment and binding?

In this section, we present a faithful interpretation for the no-go theorem, considering all physical systems appearing in a general bit commitment protocol. The similarity can be applied to oblivious transfer protocols. This interpretation will clarify the troubles with the two points:

- *Classical computations with secrets*: We show that EPR attacks of Alice is general in spite of the fact that honest Bob really uses classical secret variables and does the measurements in his computation. This interpretation, inspired from Lo's arguments in [Lo97], is simpler and more accessible than [Bub01b, Che06]. Moreover, our detailed interpretation leads to the possibility of a mental game on Bob's secrets when the number of values of these secrets is very large in comparison with the concealment parameter, cf. Section 7.3.

- *Classical communications*: We show that the security and the cheating can be analyzed for a purified protocol in a global view considering a macroscopic channel for transmitting classical message within the concepts of decoherence in quantum measurements.

This purified model shows a more general view on average concealment and binding than Mayers' one which considered these parameters only for individually each *history* of the protocol corresponding to one quantum configuration collapsed to one classical message sequence [May97].

7.1.1 Augmented model purifying private randomness and secrets

We consider the security of quantum bit commitment with private secrets and local measurements in an augmented model which purifies all these classical variables. For simplifying, we suppose that Alice and Bob communicate only quantum information. The communication via a classical channel will be considered later.

Suppose that Alice and Bob possess two quantum machines with unlimited resource. Using these machines, Alice and Bob can realize all computations at the quantum level by the purifying action described as follows.

Suppose that following the algorithm, at some step, a user $X \in \{A, B\}$ prepares a secret value which is a random variable $|i\rangle$, chosen from a finite set $\{|1\rangle, .., |n\rangle\}$ with equal probabilities $1/n$, and introduces it to a quantum circuit that compute

$$U_X(|i\rangle_X |\psi(b)\rangle_{AB})$$

where $|\psi(b)\rangle_{AB}$ is used for the remaining quantum system of the protocol. This probabilistic computation creates in fact a quantum statistical ensemble of possible configurations: $\{1/n, U_X(|i\rangle_X |\psi(b)\rangle_{AB})\}$. User X can instead prepare the entangled state

$$\sum_{i=1}^{n} \sqrt{1/n}\, |i\rangle_X |i\rangle_{D_X}\,, \tag{7.3}$$

keeps the quantum dice D_X for the purification and uses part X for the quantum algorithm as in the honest case. The computation is then kept at the quantum level

$$\sum_{i=1}^{n} \sqrt{1/n}\, |i\rangle_{D_X} U_X(|i\rangle_X |\psi(b)\rangle_{AB}).$$

Suppose that at some steps, a user $X \in \{A, B\}$ has to measure the quantum state $|\psi(b)\rangle_{AB}$ by an apparatus with n degrees of freedom. According to the output $i \in \{1, .., n\}$ and the collapsed state $|\psi_i(b)\rangle_{AB}$ with probability $p_b(i)$, this user realizes a quantum computation U_X controlled by i, i.e. he/she produces a state $|i\rangle_X |\psi_i(b)\rangle_{AB}$ for $i = 1, ..., n$, and applies $U_X(|i\rangle_X |\psi_i(b)\rangle_{AB})$. The user can instead introduce a n-dimension quantum system in X, and a n-dimension quantum dice in D_X for the purification. He couples these with $|\psi(b)\rangle_{AB}$ and transforms them to

$$\sum_{i=1}^{n} \sqrt{p_b(i)}\, |i\rangle_{D_X} |i\rangle_X |\psi_i(b)\rangle_{AB}\,, \tag{7.4}$$

Then he applies U_X to the system in $\mathcal{H}_X$ as in the honest case, i.e. the output will be

$$\sum_{i=1}^{n} \sqrt{p_b(i)}\, |i\rangle_{D_X} U_X(|i\rangle_X |\psi_i(b)\rangle_{AB}).$$

The above behaviors can be seen as semi-honest. Such semi-honest actions are not detectable because the density matrices of all systems are the same as in a honest scheme, and must be allowable because the both users have quantum machines with unlimited resource. In fact, each user respects the specified algorithm but keeps *the multiverse* of the computations corresponding to private classical variables [Deu].

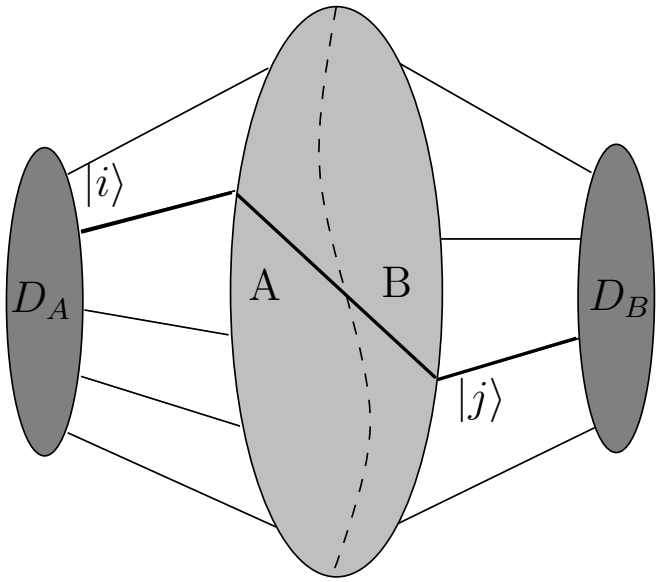

Figure 7.1: Global model purifying private classical variables

Therefore, the joint computation is an unitary evolution acting on $\mathcal{H}_{D_A} \otimes \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{D_B}$ where D_A, D_B are Alice and Bob's dices which are secret and do not appear in the execution of the protocol for honest users. The configuration at any moment can be expressed as

$$|\Psi(b)\rangle = \sum_{i,j} \sqrt{p_b(i,j)}\, |i\rangle_{D_A} |j\rangle_{D_B} |\psi_{i,j}(b)\rangle_{AB} \tag{7.5}$$

where i, j represent all possible values of classical secrets and measurement results that Alice and Bob would have produced, and $|\psi_{i,j}(b)\rangle_{AB}$ is the collapsed quantum state according to the classical values i at Alice location and j at Bob location when both are honest cf. Figure 7.1.

But the users can throw their dices to the quantum machines and fully control them as normal computational system in A, B. Then, the protocol must be concealing against this purification because D_B is fully controlled by Bob's machine, i.e:

$$\rho^{B,D_B}(0) = \rho^{B,D_B}(1) \tag{7.6}$$

where $\rho^{B,D_B}(0) = tr_{A,D_A}(|\Psi(0)\rangle \langle\Psi(0)|)$, $\rho^{B,D_B}(1) = tr_{A,D_A}(|\Psi(1)\rangle \langle\Psi(1)|)$.

Then, as exposed in Section 4.4.1, the theorem for the purified two-party system

assumes that Alice finds a cheating unitary transformation acting in $\mathcal{H}_A \otimes \mathcal{H}_{D_A}$ such that

$$U_A(|\Psi(1)\rangle) = |\Psi(0)\rangle .$$

The most common feeling is that, Bob may not necessarily follow the purified scheme. When honest Bob really does the measurements and uses classical random secrets, the two-party entanglement is destroyed. For the sake of simplicity, we throw the dices in D_A to A, and the purified state can be expressed as $|\Psi(b)\rangle = \sum_{j=1}^{N} \sqrt{p_b(j)}\, |j\rangle_{D_B} |\psi_j(b)\rangle_{AB}$. According to his classical private values $j \in \{1, .., N\}$, the global purified state is projected into the collapsed states $|\psi_j(b)\rangle_{AB}$ which may not be known to Alice. Alice could not figure out the corresponding cheating transformation.

However, if Bob does not purify his computations by throwing D_B away, he has no advantage. In any way, we cannot weaken the condition in Eq. (7.6), and because $\sqrt{p_b(j)}\, |\psi_j(b)\rangle = {}_{D_B}\langle j|\, \Psi(b)\rangle$, the transformation U_A is universal for all of Bob's secrets, i.e.

$$U_A(|\psi_j(1)\rangle) = |\psi_j(0)\rangle . \tag{7.7}$$

Even in a non-ideal case where $F(\rho^{B,D_B}(0), \rho^{B,D_B}(1)) = 1 - \epsilon$, as shown in Section 4.4.1, there exists a purification $|\Psi'(0)\rangle$ of $\rho^{B,D_B}(1)$ satisfying $|\, \langle \Psi'(0)|\, \Psi(0)\rangle\, | = 1 - \epsilon$, and Alice can find U_A:

$$\begin{aligned} \big|\Psi'(0)\big\rangle = U_A(|\Psi(1)\rangle) &= \sum_j \sqrt{p_1(j)}\, |j\rangle_{D_B}\, U_A(|\psi_j(1)\rangle_{AB}) \\ &= \sum_j \sqrt{p_1(j)}\, |j\rangle_{D_B} \big|\psi'_j(0)\big\rangle_{AB} \end{aligned}$$

Alice can use this unitary transformation to cheat. Here, in spite of the fact that there may exist some classical output j with it, Alice fails to cheat because $|\, \langle \psi_j(0)|\, \psi'_j(0)\big\rangle\, | \ll 1$, but the probability of producing such classical value j must be small and the average of Alice's possibility of success when Bob is honest can be measured by:

$$\begin{aligned} \sum_j \sqrt{p_0(j)}\sqrt{p_1(j)}\, \big|\big\langle \psi'_j(0)\big|\, \psi_j(0)\big\rangle\big| &\geq |\, \big\langle \Psi'(0)\big|\, \Psi(0)\big\rangle\, | \\ &= 1 - \epsilon. \end{aligned}$$

In conclusion, if a quantum protocol with local random variables and measurements is concealing against Bob, given that Bob has an unlimitedly powerful quantum machine, then it is not binding when Alice has an unlimitedly powerful quantum machine. In fact, as all of these local classical values can be purified by quantum machine, cf. Figure 4.3, it is required to analyze the protocol in the purified two-party model where the computations become quantum deterministic. The computation with classical variables and measurements of one user is as throwing some local systems away from the global purified model, can only cause losses of information and never help that user.

However, the choice for values of secret variable is subjectively random, not objectively, i.e. user X is free to choose the secret in Eq. (7.3) as any $|i\rangle$, even as any probability distribution P for a purification $\sum_i \sqrt{P(i)}\, |i\rangle_{D_X} |i\rangle_X$. A concrete analysis of a mental game on Bob's secrets will be provided in Section 7.3.

7.1.2 Augmented model purifying classical messages

Above, we showed that local random variables and private measurements can be purified in Alice's and Bob's quantum machine. And in such a case, the bit commitment is impossible because of a property of two-party pure states. Moreover, Bob's honest strategy, that does not take the purification step, and does not help to eliminate Alice's cheating strategy that purifies all of Alice's local random variables and measurements.

However, in a general protocol, Alice has to do the measurements because of the presence of a classical channel. As measurements "can never help a cheater" [GL00], why the measurements for making classical messages do not prevent Alice from cheating?

Mayers' proof could respond to this question. By the same arguments as above, Mayers pointed out that Alice and Bob may purify all measurements except for making classical messages. And the protocol configuration is projected to a collapsed state, indexed by the exchanged classical message and then known by both Alice and Bob. The concealment and binding are then treated by the no-go theorem for bit commitment on this sub-protocol configuration which is a pure state, cf. Section 4.4.2.

In the sequel, we will interpret the classical communications in a faithful purified model by the concepts of decoherence in quantum measurements for making exchanged messages. This makes us once more return to a global model purifying all classical messages exchanged between Alice and Bob. In this model, the average parameters for concealment and binding are more relaxed than in Mayers' case, and thus more general.

It is natural to think that in reality a classical channel is coupled with the environment where the decoherence is so strong that the messages transmitted on the channel are measured by a CNOT-like gate, copied, and amplified by an infinite quantum systems in the environment, i.e. a basis qubit $|i\rangle$ becomes $|i\rangle \otimes |i\rangle_E$ [Zur91, BS98].

In [Yao95], Yao defined a quantum two-party protocol as a pair of quantum machines interacting through a quantum channel. The protocol is executed on a joint system consisting of Alice's machine $\mathcal{H}_A$, Bob's machine $\mathcal{H}_B$, and the quantum channel $\mathcal{H}_C$. The execution is alternating rounds of one-way communications. For each round, one participant $D \in \{A, B\}$ performs a unitary computation in the joint space of his private system $\mathcal{H}_D$ and the messages $\mathcal{H}_C$. The messages will be taken to the location of the other for the next round, cf. Figure 7.2.

This model has been used as a standard for analyzing quantum communications in quantum protocols, e.g. the complexity of quantum communications [Kre95, dW02] and quantum interactive proofs [Wat99]. It was also used in the Lo & Chau's proof of the insecurity of quantum protocol for bit commitment [LC97, Bub01b].

If we use Yao's model for two-party protocols, the model should be generalized as a pair of quantum machines interacting through a quantum channel *and necessarily a classical channel*. The model consists of two machines $\mathcal{H}_A, \mathcal{H}_B$, a quantum channel $\mathcal{H}_C$ for both quantum and classical messages and a trusted measurement machine M with ancillas $\mathcal{H}_E$. The measurement is in fact a CNOT-like gate whose controlling inputs are in the space of the sender's "classical messages" and targets are ancillas in the macroscopic environment space $\mathcal{H}_E$, cf. Figure 7.3. In each communication round, a participant $D \in \{A, B\}$ does an unitary computation on $\mathcal{H}_D \otimes \mathcal{H}_C$; the trusted machine applies the CNOT gate to the "classical messages" in $\mathcal{H}_C$ and the environment of the classical channel $\mathcal{H}_E$. The quantum messages

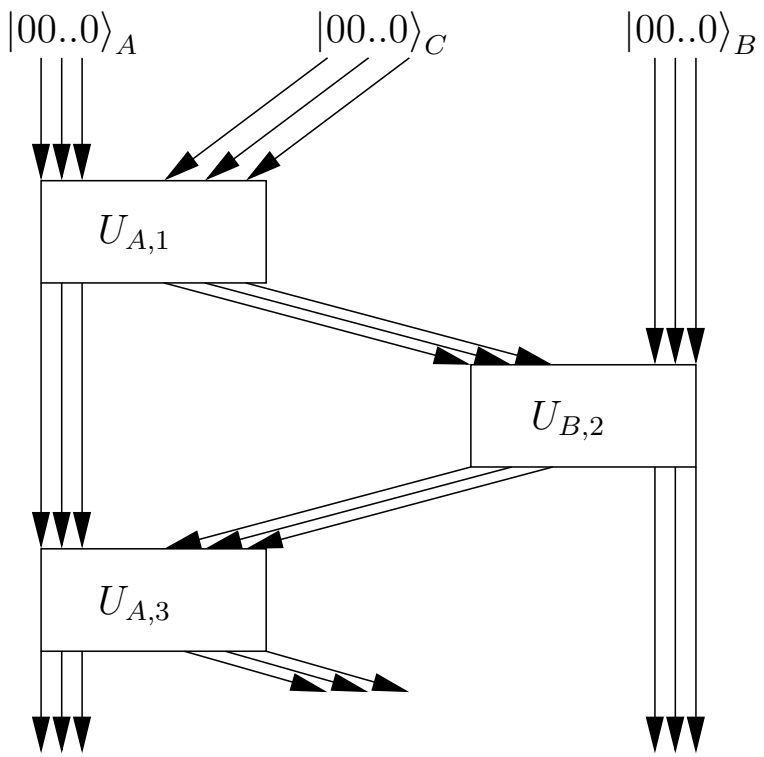

Figure 7.2: Quantum two-party model

and "classical messages" in $\mathcal{H}_C$ are taken to the other location for the next round.

But, as the quantum communications do not play an important role in the proof, it is not necessary to separate quantum communication systems from quantum computation ones. The presence of the $\mathcal{H}_C$ would be redundant. Indeed, in [LC97], the authors must assume that the channel after the commitment phase is in a pure state $|u\rangle_C$. This assumption is not evident, and may trouble the readers if provided without explication. For instance, we can use a EPR-pair channel for teleporting quantum states [BBC$^+$93], and the EPR-pair channel musts be separated from the other computational systems to guarantee that these EPR pairs are used only for the communication of quantum signals by teleportation. In [Bub01b], the channel systems C must be split into two parts in possession of Alice and Bob. We would rather faithfully consider the communication of quantum signal as quantum particles are brought from sender's machine to receiver's machine. As analyzed in Section 4.4.1, the communications of quantum messages make only repartitions of quantum systems in Alice and Bob's machines. Nevertheless, we will separately analyze the communication of classical messages via a macroscopic channel.

Suppose that the process of communication of classical message via a classical channel as follows:

1. The sender $S \in \{A, B\}$ has to measure some quantum state $|\psi\rangle_{AB}$ with an apparatus

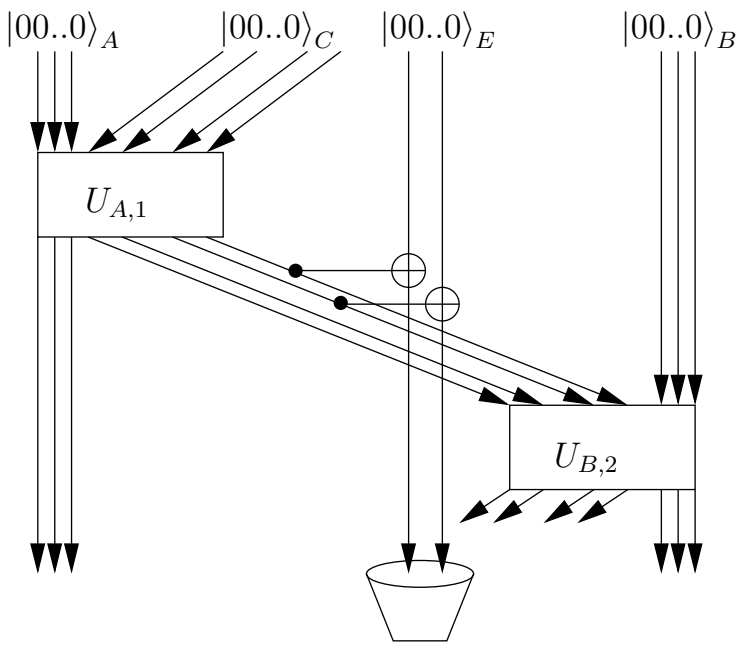

Figure 7.3: Quantum protocol with a classical channel

with n degrees. This measurement will output $i \in \{1, .., n\}$ with probability $p(i)$ and let the measured system in a state $|\psi_i\rangle_{AB}$:

$$|\psi\rangle \to \sum_i \sqrt{p(i)}\, |\psi_i\rangle_{AB} |i\rangle_S |i\rangle_{E,S}$$

where $\mathcal{H}_{E,S}$ is for the macroscopic part in the measurement device lost to the environment that causes the impurity of sender's state.

2. The sender sends the signal i via a macroscopic channel where the signal can be infinitely amplified by the environment E:

$$|i\rangle_S \to |i\rangle_S \otimes |i\rangle_E .$$

3. The signal is amplified, and propagates to the receiver's device, where the corresponding quantum state $|i\rangle$ will be generated for the receiver's quantum machine $R = \{A, B\} \setminus \{S\}$:

$$|i\rangle_E \to |i\rangle_E \otimes |i\rangle_R .$$

Therefore, we can see this process acts on a pure state, but in a larger space covering Alice's, Bob's machine and the environmental systems amplifying the signals:

$$|\psi\rangle_{AB} |0\rangle_{S,R,E*} \to \sum_{i=1}^{n} \sqrt{p(i)}\, |i\rangle_S |i\rangle_{E*} |i\rangle_R |\psi_i\rangle_{AB}$$

where $E*$ denotes all systems of the environment, and S, R denote the controllable quantum systems in Alice's and Bob's machines. The initial states of systems storing the classical messages in this process are not important, and denoted by $|0\rangle_{S,R,E*}$. So, by introducing the environment systems $E*$, the execution of the protocol is seen as a deterministic unitary evolution of the global three-party state lying in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{E*}$.

Here, $\mathcal{H}_{E*}$ is not controlled by any participant, and the configurations of the protocol are not pure states lying in a two-party space for quantum systems in Alice' and Bob's machines anymore. Nevertheless, it's a three-party model where the systems in $E*$ play a passive role via the CNOT gates, make us have to leave the purified model, cf. Figure 4.3 and turn back to the superoperator model, cf. Figure 4.2.

Therefore, the protocol is seen as a deterministic computation on a three-party space and the configuration of the protocol at any moment can be described by a known pure state in the form of

$$|\Psi(b)\rangle = \sum_{i=1}^{N} \sqrt{p_b(i)}\, |i\rangle_{E*} |i\rangle_A |i\rangle_B |\psi_i(b)\rangle_{AB} \tag{7.8}$$

where i is any possible classical message, and $|i\rangle_A, |i\rangle_B$ appear for the fact that Alice and Bob can duplicate and keep a record of the classical messages forever in their machines.

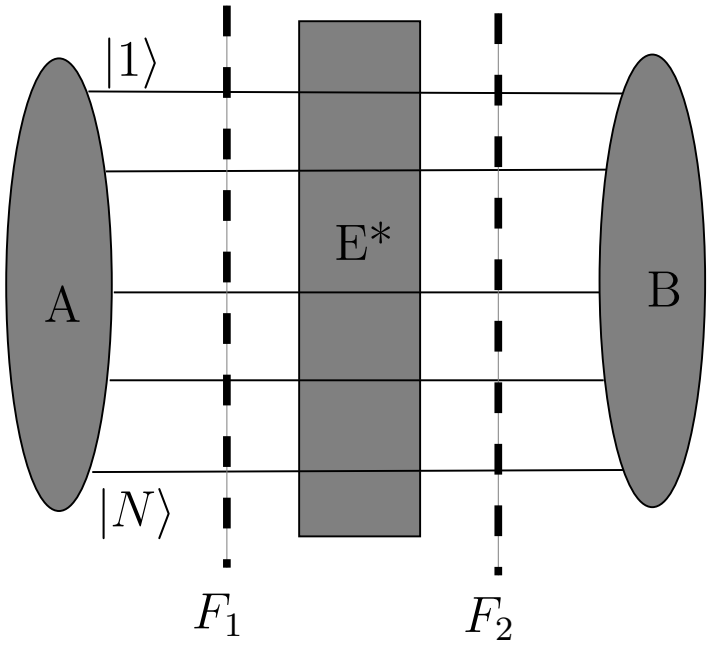

Figure 7.4: Entanglement connections via classical messages

For the security on Bob's side, the protocol has to assume

$$F(\rho^B(0), \rho^B(1)) \geq 1 - \epsilon$$

where $\rho^B(b) = tr_{E*}(tr_A(|\Psi(b)\rangle \langle\Psi(b)|))$.

Of course, Alice can only control the quantum systems in his machine $\mathcal{H}_A$ and

$$F(\rho^{B,E*}(0), \rho^{B,E*}(1)) \leq F(\rho^B(0), \rho^B(1)) \tag{7.9}$$

where $\rho^{B,E*}(b) = tr_A(\rho(b))$. The inequality happens when information are lost during communication via the classical channel. Unfortunately, the environment has only honestly amplified the signals and the equality is obtained:

$$\begin{aligned} F(\rho^{B,E*}(0), \rho^{B,E*}(1)) &= F(\rho^B(0), \rho^B(1)) \\ &\geq 1 - \epsilon \end{aligned}$$

because in the description of $|\Psi(b)\rangle$, $|i\rangle_{E*}$ is exactly the same as $|i\rangle_A$. Therefore, there exists an unitary transformation U_A such that

$$|\langle\Psi(0)| U_A |\Psi(1)\rangle| \geq 1 - \epsilon$$

In Figure 7.4, we represent each entanglement connection via a classical message i by a line. The frontier F_1 at the limit of Alice's control gives Bob the same information as at F_2. The classical channel is noiseless and does not help Bob, cf. Eq. (7.9). We can recall that a noisy channel could enable us to build unconditionally secure primitives [Cré97, CMW04].

The above purified model exists only if we accept the concept of decoherence that leads to the *Many Worlds Interpretation* of quantum mechanics where the pure global state exists as the multiverse of classical realms corresponding to the collapsed state [Sch04]. This pure state may not exist in reality according to the *Copenhagen Interpretation*, because Alice and Bob should be in one of N situations, provided a collapsed state $|i\rangle_A |i\rangle_B |\psi_i(b)\rangle_{AB}$ with the corresponding probabilities $p_b(i)$, i.e. we are provided instead a statistical ensemble $\{p_b(i), |i\rangle_A |i\rangle_B |\psi_i(b)\rangle_{AB}\}$.

In that case, Alice's average cheating possibility over all occurrence of exchanged classical messages can be measured by

$$\begin{aligned} \sum_i^N \sqrt{p_0(i)p_1(i)} |\langle\psi_i(0)| \langle i| U_A |i\rangle |\psi_i(1)\rangle| &\geq |\langle\Psi(0)| U_A |\Psi(1)\rangle| \\ &\geq 1 - \epsilon \end{aligned}$$

We see that these collapsed states are the same as $|\psi_{b,\gamma}\rangle$ in Mayers' version for $i = \gamma$. The above average cheating possibility of Alice suggests to extended the average concealment for the protocol from Mayers' individual collapsed protocols as

$$CONC' = \sum_\gamma \sqrt{p_0(\gamma)p_1(\gamma)} F_\gamma$$

Of course, if we could measure the average concealment as

$$\begin{aligned} CHEAT' &= \sum_\gamma \sqrt{p_0(\gamma)p_1(\gamma)} |\langle\psi_{0,\gamma}| U_{A,\gamma} |\psi_{1,\gamma}\rangle| \\ &= \sum_\gamma \sqrt{p_0(\gamma)p_1(\gamma)} F_\gamma \end{aligned}$$

Moreover, as a standard, the concealment can be measured by

$$CONC = F\left(\sum_{\gamma} p_0(\gamma)\rho_{\gamma}^{B}(0), \sum_{\gamma} p_1(\gamma)\rho_{\gamma}^{B}(1)\right).$$

Normally $CHEAT' \leq CONC$ ([NC04] - theorem 9.7), but as Bob keeps a record of classical message γ in his quantum state $\rho_{\gamma}^{B}(b)$ the two measures of concealment are identical $CONC' = CONC$ and then $CHEAT' = CONC$.

Logically, we are allowed to reduce this three-party model to a pure quantum two-party model by making $|i\rangle_{E*}$ disappear as this is only a redundant copy of $|i\rangle_A |i\rangle_B$. However, this reduced pure quantum two-party model only emulates the real protocols *logically*, *not physically*. The reduction could not so be evident without a physical interpretation.

7.1.3 Summary

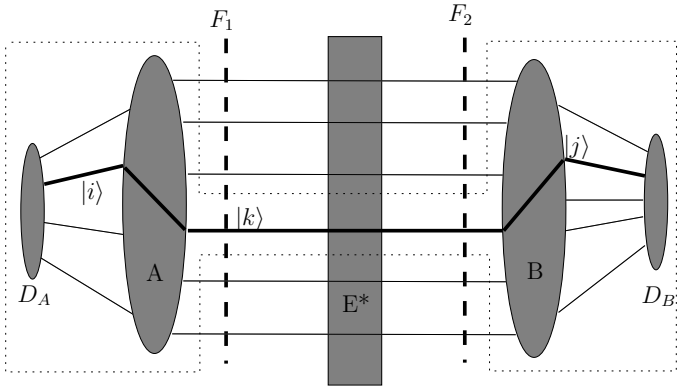

Figure 7.5: The global purified model

In summary, the global purified model which was obtained by the purification of local random variables, cf. Eq. (7.5), and exchanged classical messages, cf. Eq. (7.8), can be illustrated as in Figure 7.5 which describes the configuration of the protocol at any given moment. This configuration is in a pure state:

$$|\Psi(b)\rangle = \sum_{k,i,j} \sqrt{p_b(k,i,j)}\, |k\rangle_{ABE*} |i\rangle_{D_A} |j\rangle_{D_B} |\psi_{k,i,j}\rangle_{AB}$$

The execution of the protocol is a sequence of deterministic unitary transitions between successive configurations. It is a parallel execution of many honest schemes. For instance, the real configuration of the protocol corresponding to Alice's private outcome i, Bob's private outcome j and exchanged classical message k is represented by the bold line in the figure.

As Alice and Bob have the possibility to keep their dices in their quantum machines, we would throw D_A to A and D_B to B and the no-go theorem is applied to the model as analyzed above.

Note that, if the purification of local variables $|i\rangle$ and $|j\rangle$ is really possible as Alice's and Bob's throw the private dices D_A, D_B to their quantum machines, the purification of exchanged classical messages $|k\rangle$ is more abstract. It is a quantum parallelism of collapsed counterparts corresponding to exchanged classical messages as in Mayers' interpretation [May97]: the configuration corresponding to the classical message k lies in the region marked by the dot line in Figure 7.5.

Nevertheless, this global purification describes the real execution of a protocol if the Nature follows the theory of *Decoherence* and *Many Worlds Interpretation*. In any way, it is a convenient model for analyzing the average values of concealment and binding of general protocols with classical communications.

7.2 Extensions of the No-go Theorems

We fall into the same situation as in the classical world since classical protocols were also impossible. We could be satisfied to use a trusted third party for unconditionally secure computations. It is trivial when we have a trusted third party for implementing these protocols. For instance, in an oblivious transfer protocol, Alice sends b_0, b_1 and Bob sends c to Trent who is honest; Trent sends b_c to Bob. We call this as a *trusted two-party oracle* model, i.e. we construct a trusted two-party circuit for any desired computation, with some inputs from Alice and Bob, and some outputs back to Alice and Bob. The execution time of the computation done by the oracle is an elementary unit, and we can consider as it immediately returns the results to the participants.

In this Section, we present an extension of the impossibility of quantum bit commitment and oblivious transfer for some particular two-party oracle models.

7.2.1 Short-Term Oracle

Definition 7.1. *We define a* Short-Term Oracle *(ST-O) as a trusted two-party oracle that implements any specified algorithm, using some local variables. At the end of the computation, the oracle splits all the final values of all variables, including local one, and sends back one part to Alice, one part to Bob.*

For instance, a simple classical circuit for oblivious transfer with 2 input wires from Alice for $\{b_0, b_1\}_A$, 2 input wires from Bob for $\{c, x\}_B$, is built with logic gates for the transition

$$\{b_0, b_1\}_A\{c, 0\}_B \rightarrow \{b_0, b_1\}_A\{c, b_c\}_B \tag{7.10}$$

and redirects output wires A to Alice, B to Bob. The input wire initialized to 0 is for Bob storing the received bit.

A quantum ST-O is illustrated as in Figure 7.6: it receives quantum signal for inputs from Alice and Bob; initializes necessary local variables to $|0\rangle$; applied the required computation to these inputs; and at the end splits all of the outputs, including the local variables, into two parts, redirects one part to Alice, and one part to Bob.

We can extend the no-go theorems to a more general quantum quantum based on ST-O:

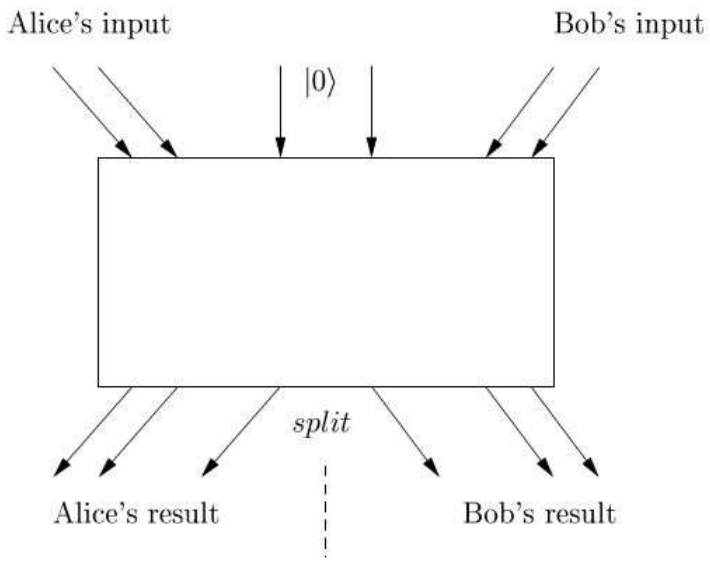

Figure 7.6: The quantum Short-Term Oracle

Theorem 7.1 (Extension of no-go theorems)**.** *We cannot build secure Quantum bit commitment, oblivious transfer protocol based quantum ST-Os.*

Proof. (Sketch). In fact, when the oracle uses only pure states as local input, and immediately, splits and sends all of the qubits that participate to the computations to Alice and Bob, the global state at any considered moment is in some known pure state, according to the algorithm, in a two-party space relating only Alice and Bob sides. Therefore, the no-go theorems remain valid.

For example, we prove the impossibility of one-sided secure computation. As shown in Section 7.1, the average of security and cheating possibility of general protocols with random variables, secrets variables, and classical communications, could be analyzed in a deterministic purified model. It is then sufficient to prove the theorem for this reduced model.

We start with Eq. (4.4). Attaching a pure state $|0\rangle_{A'B'}$, locally prepared by the oracle, the initial state is

$$\left|u'\right\rangle_{in} = \frac{1}{\sqrt{n}} \sum_i |i\rangle_P \otimes |i\rangle_A \otimes |j_1\rangle_B \otimes |0\rangle_{A'B'} .$$

At the end of the computation, with help of the oracle, the combined system is in state

$$|v_{j1}\rangle = \frac{1}{\sqrt{n}} \sum_i |i\rangle_P \otimes U(|i\rangle_A \otimes |j_1\rangle_B \otimes |0\rangle_{A'B'})$$

where system A' is set to A, system B' is set to B after the split. Therefore, the remaining arguments of Lo's proofs can be followed, cf. Section 4.4.1. □

7.2.2 Trivial Oracle Model

In our interpretation of MLC nogo theorems, we discovered that quantum bit commitment and oblivious transfer are impossible even with the presence of an uncontrollable third party systems such as the macroscopic channel. The macroscopic channel for Alice and Bob communicating classical information plays the role of an trusted oracle which publicly measures the quantum states in Alice and Bob machines. The measurements for making classical messages are indeed non information-erasing in the joint view of Alice and Bob. We can extend the no-go theorems to quantum protocols based on such trivial oracle.

Definition 7.2. *We define a Quantum Trivial Oracle as a trusted two-party oracle which can implement the computation of any two-party function. The oracle can be coupled with an environment quantum system O uncontrollable by Alice and Bob. The oracle does any measurement in public, i.e whenever the oracle throws some information to O, it makes two copies of the information, and sends one to Alice, one to Bob.*

Then, more generally:

Theorem 7.2 (Extension of no-go theorems)**.** *We cannot build secure Quantum bit commitment, oblivious transfer protocol based on Quantum Trivial Oracles.*

For the sketch, we can throw all of systems in O to the global third party environment $E*$, then the global configuration of any protocol based on trivial oracles at any moment is of the same form as Eq. (7.8):

$$|\Psi\rangle = \sum_{i=1}^{N} \sqrt{p_b(i)}\, |i\rangle_{E*} |i\rangle_A |i\rangle_B |\psi_i\rangle_{AB} \tag{7.11}$$

In this three-party model involving Alice's machine, Bob's machine and the systems in $E*$, at any time the global state of a protocol can be described by the form as in Eq. (7.11), and thus

- The systems in $E*$ do not hide information from Bob in a bit commitment scheme. It could be then seen as a two-party model $\mathcal{H}_A \otimes (\mathcal{H}_{E*} \otimes \mathcal{H}_B)$ where $\mathcal{H}_{E*} \otimes \mathcal{H}_B$ is for what Bob can learn about Alice's secret and $\mathcal{H}_A$ is for what Alice can fully control to cheat.

- The systems in $E*$ do not hide information from Alice in an oblivious transfer scheme. It could be then seen as a two-party model $(\mathcal{H}_A \otimes \mathcal{H}_{E*}) \otimes \mathcal{H}_B$ where $\mathcal{H}_A \otimes \mathcal{H}_{E*}$ is for what Alice can learn about Bob's secret and $\mathcal{H}_B$ is for what Alice can fully control to cheat.

7.2.3 A case-study

Let verify a quantum ST-O for implementing oblivious transfer protocol with some familiar quantum gates.

Inspired from Bennett et al. [BDSW96], we use the notations:

$$\begin{aligned}
\left|\widetilde{00}\right\rangle &= |\Phi+\rangle = (|00\rangle + |11\rangle)/\sqrt{2},\\
\left|\widetilde{01}\right\rangle &= |\Phi-\rangle = (|00\rangle - |11\rangle)/\sqrt{2},\\
\left|\widetilde{10}\right\rangle &= |\Psi+\rangle = (|01\rangle + |10\rangle)/\sqrt{2},\\
\left|\widetilde{11}\right\rangle &= |\Psi-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}.
\end{aligned}$$

Our ST-O uses three local qubits. The first and the second local qubits are prepared in entangled state $\left|\widetilde{00}\right\rangle$. The third qubit is initialized to $|0\rangle$.

Let b_0, b_1 be the two bits that Alice want to send and c be Bob's choice. The trusted party does a controlled π rotation $R_{b_0 b_1}$ on the first qubit, according to b_0, b_1:

$$R_{00} = I, R_{01} = \sigma_z, R_{10} = \sigma_x, R_{11} = \sigma_y.$$

The first and second qubits are obtained in state $\left|\widetilde{b_0 b_1}\right\rangle$. Next, in case $c = 1$ the trusted party applies the bilateral $\pi/2$ rotation B_y to the first and second qubits [BDSW96]:

$$\begin{aligned}
\left|\widetilde{00}\right\rangle &\rightarrow_{B_y} \left|\widetilde{00}\right\rangle,\\
\left|\widetilde{01}\right\rangle &\rightarrow_{B_y} \left|\widetilde{10}\right\rangle,\\
\left|\widetilde{10}\right\rangle &\rightarrow_{B_y} \left|\widetilde{01}\right\rangle,\\
\left|\widetilde{11}\right\rangle &\rightarrow_{B_y} \left|\widetilde{11}\right\rangle.
\end{aligned}$$

The trusted party applies then the CNOT gates computing the parity of the first and the second qubits and the target is the third qubit. Then, the trusted party undoes the rotation B_y controlled by c and the bilateral rotation $R_{b_0 b_1}$. The computation done by the ST-O is a quantum circuit acting on 6 qubits: two for Alice's inputs, three for the local qubits, one for Bob's input. Finally the ST-O splits the outputs ends back the two first qubits to Alice and four last qubits to Bob, cf. Figure 7.7.

Simply speaking, if Alice and Bob are subjected to send b_0, b_1, c to T as classical signals $|b_0\rangle, |b_1\rangle, |c\rangle \in \{|0\rangle, |1\rangle\}$, the quantum ST-O implements a O-OT gate:

$$\begin{aligned}
|b_0 b_1\rangle_A \left|\widetilde{00}\right\rangle_T |0\rangle_T |c\rangle_B \quad &\rightarrow_{R_{b_0 b_1}} \quad |b_0 b_1\rangle_A \left|\widetilde{b_0 b_1}\right\rangle_T |0\rangle_T |c\rangle_B\\
&\rightarrow_{B_y} \quad |b_0 b_1\rangle_A \left|\widetilde{b_c b_{1-c}}\right\rangle_T |0\rangle_T |c\rangle_B\\
&\rightarrow_{CNOTs} \quad |b_0 b_1\rangle_A \left|\widetilde{b_c b_{1-c}}\right\rangle_T |b_c\rangle_T |c\rangle_B\\
&\rightarrow_{B_y, R_{b_0 b_1}} \quad |b_0 b_1\rangle_A \left|\widetilde{00}\right\rangle_T |b_c\rangle_T |c\rangle_B\\
&\rightarrow_{split} \quad |b_0 b_1\rangle_A \left|\widetilde{00}\right\rangle_B |b_c\rangle_B |c\rangle_B.
\end{aligned}$$

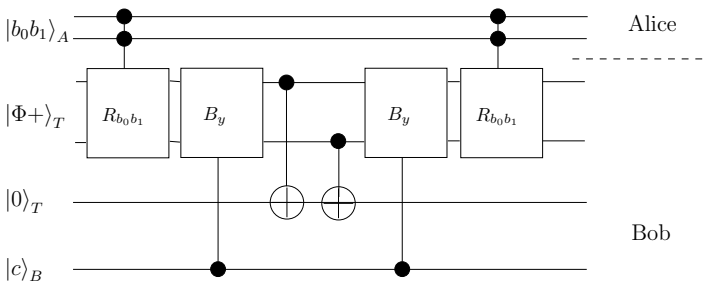

Figure 7.7: A Short-term Oracle for O-OT protocol

In case Alice and Bob communicate with ST-O via quantum channels, they can send quantum inputs directly. Suppose that Alice prepares inputs as a superposition

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\cdot$$

The global input state is then

$$|in\rangle = \frac{1}{2}(|00\rangle_A + |01\rangle_A + |10\rangle_A + |11\rangle_A)\left|\widetilde{00}\right\rangle_T |0\rangle_T |c\rangle_B .$$

If Bob sends $|c\rangle = |0\rangle$ then the computation is

$$\begin{aligned}
|in\rangle \quad &\rightarrow_{R_{b_0b_1}} \quad \frac{1}{2}\left[|00\rangle_A \left|\widetilde{00}\right\rangle_T + |01\rangle_A \left|\widetilde{01}\right\rangle_T + |10\rangle_A \left|\widetilde{10}\right\rangle_T + |11\rangle_A \left|\widetilde{11}\right\rangle_T\right] |0\rangle_T |0\rangle_B \\
&\rightarrow_{CNOTs} \quad \frac{1}{2}\left[|00\rangle_A \left|\widetilde{00}\right\rangle_T |0\rangle_T + |01\rangle_A \widetilde{01}_T |0\rangle_T + |10\rangle_A \left|\widetilde{10}\right\rangle_T |1\rangle_T + |11\rangle_A \left|\widetilde{11}\right\rangle_T |1\rangle_T\right] |0\rangle_B \\
&\rightarrow_{B_y,R_{b_0b_1}} \quad \frac{1}{2}\left[(|00\rangle_A + |01\rangle_A)\left|\widetilde{00}\right\rangle_T |0\rangle_T + (|10\rangle_A + |11\rangle_A)\left|\widetilde{00}\right\rangle_T |1\rangle_T\right] |0\rangle_B \\
&\rightarrow_{split} \quad \frac{1}{2}\left[(|00\rangle_A + |01\rangle_A)\left|\widetilde{00}\right\rangle_B |0\rangle_B + (|10\rangle_A + |11\rangle_A)\left|\widetilde{00}\right\rangle_B |1\rangle_B\right] |0\rangle_B .
\end{aligned}$$

If Bob sends $|c\rangle = |1\rangle$ then the computation is

$$\begin{aligned}
|in\rangle \quad &\rightarrow_{R_{b_0b_1}} \quad \frac{1}{2}\left[|00\rangle_A \left|\widetilde{00}\right\rangle_T + |01\rangle_A \left|\widetilde{01}\right\rangle_T + |10\rangle_A \left|\widetilde{10}\right\rangle_T + |11\rangle_A \left|\widetilde{11}\right\rangle_T\right] |0\rangle_T |1\rangle_B \\
&\rightarrow_{B_y} \quad \frac{1}{2}\left[|00\rangle_A \left|\widetilde{00}\right\rangle_T + |01\rangle_A \left|\widetilde{10}\right\rangle_T + |10\rangle_A \left|\widetilde{01}\right\rangle_T + |11\rangle_A \left|\widetilde{11}\right\rangle_T\right] |0\rangle_T |1\rangle_B \\
&\rightarrow_{CNOTs} \quad \frac{1}{2}\left[|00\rangle_A \left|\widetilde{00}\right\rangle_T |0\rangle_T + |01\rangle_A \left|\widetilde{10}\right\rangle_T |1\rangle_T + |10\rangle_A \left|\widetilde{01}\right\rangle_T |0\rangle_T + |11\rangle_A \left|\widetilde{11}\right\rangle_T |1\rangle_T\right] |1\rangle_B \\
&\rightarrow_{B_y,R_{b_0b_1}} \quad \frac{1}{2}\left[(|00\rangle_A + |10\rangle_A)\left|\widetilde{00}\right\rangle_T |0\rangle_T + (|01\rangle_A + |11\rangle_A)\left|\widetilde{00}\right\rangle_T |1\rangle_T\right] |1\rangle_B \\
&\rightarrow_{split} \quad \frac{1}{2}\left[(|00\rangle_A + |10\rangle_A)\left|\widetilde{00}\right\rangle_B |0\rangle_B + (|01\rangle_A + |11\rangle_A)\left|\widetilde{00}\right\rangle_B |1\rangle_B\right] |1\rangle_B .
\end{aligned}$$

The partial configurations are then

$$\rho_0^A = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & 0 & 0 \\ \frac{1}{4} & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & \frac{1}{4} & \frac{1}{4} \end{pmatrix}, \quad \rho_1^A = \begin{pmatrix} \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} \end{pmatrix}$$

We see that the reduced density matrices at Alice's location are different for the two cases, $\rho_0^A \neq \rho_1^A$, and so c is not secure against Alice. For instance, Alice can measure the first and the second qubit with the projection $(\langle 00| - \langle 01| + \langle 10| - \langle 11|)/2$, and has a nonzero probability of getting a positive result when $c = 1$.

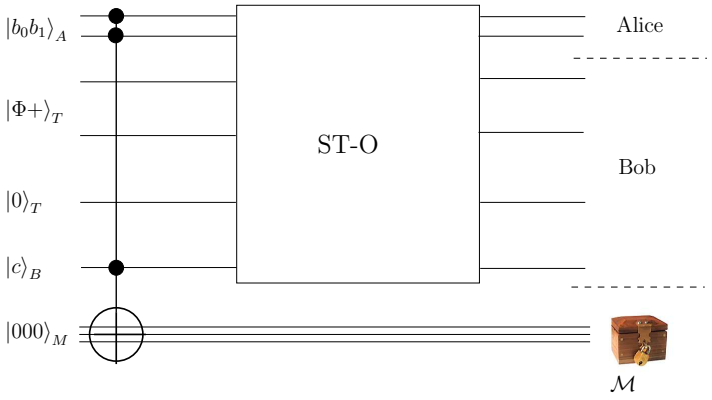

Figure 7.8: Classical channels hiding information

We reconsider the case where Alice and Bob communicate with the ST-O via classical channels. It is done as though the quantum channels are equipped with measurement devices as in Figure 7.8. The inputs will be measured and projected onto the computational basis.

Using the defined model for the classical channel, Alice sends her inputs through CNOT gates whose targets are in the measurement machine M of the classical channel between Alice and the ST-O. The output is entangled with M. In case Alice prepares any superposition of inputs $a|00\rangle + b|01\rangle + c|10\rangle + d|1\rangle$, the final states of the computations for $c = 0$ and $c = 1$ are

$$|out_0\rangle = (a|00\rangle_A|00\rangle_M + b|01\rangle_A|01\rangle_M)\left|\widetilde{00}\right\rangle_B|00\rangle_B + (c|10\rangle_A|10\rangle_M + d|11\rangle_A|11\rangle_M)\left|\widetilde{00}\right\rangle_B|10\rangle_B,$$
$$|out_1\rangle = (a|00\rangle_A|00\rangle_M + b|10\rangle_A|10\rangle_M)\left|\widetilde{00}\right\rangle_B|01\rangle_B + (c|01\rangle_A|01\rangle_M + d|11\rangle_A|11\rangle_M)\left|\widetilde{00}\right\rangle_B|11\rangle_B.$$

The reduced matrices of three qubits at Alice location are gained by tracing out M part and B part, and become

$$\rho_0^B = \rho_1^B = \begin{pmatrix} |a|^2 & 0 & 0 & 0 \\ 0 & |b|^2 & 0 & 0 \\ 0 & 0 & |c|^2 & 0 \\ 0 & 0 & 0 & |d|^2 \end{pmatrix}.$$

Thus, the protocol is secure against Alice. By the similar analysis, we see that the protocol is secure against Bob cheating. In fact, the decoherence on the classical channel between Alice and the ST-O creates an entanglement with the environment M which hides information from Bob, while the decoherence on the classical channel between Bob and the ST-O creates an entanglement with the environment M which hides information from Alice. The classical channels do not public measurements any more.

7.2.4 Coin Flipping based protocols

As a corollary of Theorem 7.2, we conclude that

Corollary 7.1. *Coin Flipping based Quantum Bit Commitment and Quantum Oblivious Transfer are impossible.*

In [Ken99], Kent showed a similar result. In his paper, he established a relativist model to implement coin flipping. With an assumed quantum trusted party, we made the model more comprehensible from a non-relativist point of view.

Proof. In an indirect manner, we can state that coin flipping is weaker than bit commitment and oblivious transfer. Indeed, we suppose that Alice and Bob have access to a ST-O that creates a pair of qubits in Bell state $|\Phi+\rangle = (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)/\sqrt{2}$ and sends each part to a user. With such a ST-O, Alice and Bob have a fair quantum coin that can realize classical coin flipping: Alice and Bob measure $|\Phi+\rangle$ in the same basis $\{|0\rangle, |1\rangle\}$ to share a random bit. However, quantum bit commitment and oblivious transfer are not realizable with this ST-O, as shown by Theorem 7.2.

We make here a more direct proof for protocols based on classical coin flipping. Suppose that Alice and Bob have access to a subroutine that can generate classical random coins and send two copies to Alice and Bob. The classical coins is then an probabilistic ensemble of $|0\rangle_A |0\rangle_B, |1\rangle_A |1\rangle_B$ with probabilities $1/2, 1/2$:

$$\rho^{AB} = (|0_A 0_B\rangle \langle 0_A 0_B| + |1_A 1_B\rangle \langle 1_A 1_B|)/2$$

The coins can be represented by a pure state in an augmented model as though they are entangled with a third-party system T.

$$|C\rangle = \sqrt{1/2}(|0\rangle_A |0\rangle_B |0\rangle_T + |1\rangle_A |1\rangle_B |1\rangle_T)$$

Suppose that a quantum protocol implemented between Alice and Bob requires Alice and Bob to share random coins at some steps. Recall that just before the first call to the subroutine, the quantum configuration of the protocol, realized by normal communication between Alice and Bob, is in a state of the penalized form $|\Psi\rangle = \sum_{i=1}^{N} \sqrt{p_b(i)} |i\rangle_{E*} |i\rangle_A |i\rangle_B |\psi_i\rangle_{AB}$, cf. Eq. (7.8). After receiving a coin, the configuration becomes

$$|\Psi\rangle \otimes |C\rangle = \sum_{i=1..N, j=0..1} \sqrt{p_b(i)/2} |ij\rangle_{E*} |ij\rangle_A |ij\rangle_B |\psi_i\rangle_{AB}$$

where T is thrown to $E*$. We see that this formula is also of the penalized form, cf. Eq. (7.11). Therefore, by induction, with any successive unitary transformation on A, B ands

request for random coins to the oracle, the global configuration of the protocol remains in the penalized form. Therefore, quantum bit commitment and oblivious transfer based on coin flipping are impossible.

To one who sticks to the Copenhagen Interpretation of quantum mechanics, the quantum configuration of joint computation just before a request to the coin flipping subroutine is a projected state $|\psi_i\rangle_{AB}$ which is known to Alice and Bob according to the exchanged messages i. Now, the coin flipping subroutine provides either $|0\rangle_A|0\rangle_B$ or $|1\rangle_A|1\rangle_B$ with equal probability. However, once the coins are provided, Alice and Bob know which coin they have, and the global state is accordingly a known state $|\psi_i\rangle_{AB} \otimes |0\rangle_A|0\rangle_B$ or $|\psi_i\rangle_{AB} \otimes |1\rangle_A|1\rangle_B$. And the no-go theorems can be applied to each of these collapsed pure states, as in Mayers' proof [May97]. □

7.3 Subjective Secrets and a Game on Secret Parameters ?

Recall that, in the augmented model purifying Bob's private classical variables, Bob's secret variables are analyzed by assigning to them a probability distribution, cf. Eq. (7.3), normally a flat distribution. But these variables are "subjectively" random, not "objectively" random as in a measurement in Eq. (7.4). We consider only the dices in D_B that purify these "subjectively" random variables, and the dices purifying "objectively" random results of measurements are thrown to B. D_A is also thrown to A as Alice keeps all of her dices in the quantum machine. The computational configuration in Eq. (7.5) is then

$$|\Psi(b)\rangle = \sum_{j=1}^{N} \sqrt{1/N}\,|j\rangle_{D_B}\,|\psi_j(b)\rangle_{AB}\,,$$

where N is the number of all possible values of Bob's secret variables used in the computation. The theorem for deterministic model assumes that we can find a unitary U_A for Alice cheating with threshold $1-\epsilon$:

$$\sum_j \frac{1}{N}\,|\langle\psi_j(0)|\,U_A|\psi_j(1)\rangle| \geq 1-\epsilon \tag{7.12}$$

However, in reality Bob is free to choose these variables, i.e. Bob can choose any distribution over $\{1,...,N\}$. The configuration would be in a state

$$|\Psi_\omega(b)\rangle = \sum_{j=1}^{N} \sqrt{p_\omega(j)}\,|j\rangle_{D_B}\,|\psi_j(b)\rangle_{AB}$$

where $\omega \in \Omega \subset [0,1]^N$ is for denoting the probability diffusion over $\{1,...,N\}$ created by Bob. Of course, for the security on Bob's side, the protocol must hold

$$\forall\omega, F(\rho^B_\omega(0), \rho^B_\omega(1)) \geq 1-\epsilon,$$

and then for each decision of Bob on ω, Alice has a corresponding cheating unitary transformation $U_{A,\omega}$:

$$\sum_j p_\omega(j)|\ \langle\psi_j(0)|\, U_{A,\omega}|\psi_j(1)\rangle\ | \geq |\,\langle\Psi_\omega(0)|\, U_{A,\omega}|\Psi_\omega(1)\rangle|$$
$$\geq 1-\epsilon. \tag{7.13}$$

The question is: "Is there a protocol that is secure against Bob, but Alice can not find the universal cheating unitary because of ω?"

When the protocol is ideally secure, then the answer is No, because Alice's transformation is universal, cf. Eq. (7.7). For non-ideal case, inspired from [Lo97], we treat also two following cases.

7.3.1 Case 1: $N\epsilon = \delta \ll 1$

We see that, Alice's cheating transformation for the flat distribution satisfies Eq. (7.12). Therefore, for all secret value j,

$$|\,\langle\psi_j(0)|\, U_A|\psi_j(1)\rangle| \geq 1 - N\epsilon = 1-\delta$$

and then, for any distribution used by Bob, the Alice's possibility of cheating is:

$$\sum_j p_\omega(j)|\ \langle\psi_j(0)|\, U_A|\psi_j(1)\rangle\ | \geq 1-\delta.$$

Cheung showed also a similar result [Che06].

7.3.2 Case 2: $\epsilon \ll 1 \leq N\epsilon$

It may happen that, for any transformation $U_{A,\omega}$ for Alice, there exists a distribution ω' such that Bob can detect Alice cheating with a significant probability

$$|\,\langle\Psi_{\omega'}(0)|U_{A,\omega}\,|\Psi_\omega(1)\rangle\,|$$
$$\leq \sum_j \sqrt{p_{\omega'}(j)p_\omega(j)}|\ \langle\psi_j(0)|\, U_{A,\omega}|\psi_j(1)\rangle\ |$$
$$\ll 1, \tag{7.14}$$

in contrast to Eq. (7.13). *If such a protocol exists*, satisfying both Eqs. (7.13) and (7.14), we are in a non stable game on Bob's secret variables:

- If Alice fixes a transformation $U_{A,\omega}$, then Bob can choose an distribution ω' to detect Alice's cheating with a significant probability, cf. Eq. (7.14). There may be a collection $\{\omega_1, .., \omega_k\}$ for Bob.
- But, if Bob determines his distribution ω', Alice can find a cheating transformation $U_{A,\omega'}$ with high probability of not being detected by Bob, cf. Eq. (7.13). Even if Bob

uses a random collection of distribution $\{\omega_1, .., \omega_k\}$, Alice can treat it as a pure state by considering that Bob's introduce some extra dices t:

$$|0\rangle = \sum_{t=1}^{k} \sqrt{1/k}\, |t\rangle_D \otimes |\Psi_{\omega_t}(0)\rangle$$
$$|1\rangle = \sum_{t=1}^{k} \sqrt{1/k}\, |t\rangle_D \otimes |\Psi_{\omega_t}(1)\rangle$$

And as the protocol must be secure against Bob, i.e. $F(tr_A(|0\rangle\langle 0|), tr_A(|1\rangle\langle 1|)) \geq 1-\epsilon$, Alice can find an unitary U_A^* with the average of possibility of cheating

$$\sum_j \left(\sum_{t=1}^{k} p_{\omega_t}(j)/k \right) |\, \langle\psi_j(0)|\, U_A^* |\psi_j(1)\rangle\, | \geq |\, \langle 0|\, U_A^* |1\rangle\, | \geq 1-\epsilon. \tag{7.15}$$

In fact, the cheating transformation $U_{A,\omega*}$ for $\omega*$ being the mean distribution of $\omega_1, .., \omega_k$, i.e. $p_{\omega*}(j) = \sum_{t=1}^{k} p_{\omega_t}(j)/k$, satisfies Eq. (7.15) and can be used as U_A^*.

Nevertheless, we do not know whether or not a quantum protocol exists for such a non stable mental game on secret variables, satisfying that for all distribution ω

- there exists a transformation U_A such that
$$\sum_j p_\omega(j) |\, \langle\psi_j(0)|\, U_{A,\omega} |\psi_j(1)\rangle\, | \geq 1-\epsilon$$
- and for this U_A, there exists a distribution ω' such that
$$\sum_j \sqrt{p_{\omega'}(j) p_\omega(j)} |\, \langle\psi_j(0)|\, U_{A,\omega} |\psi_j(1)\rangle\, | \ll 1.$$

7.3.3 Summary

We see that in the case where Bob has a secret S for which Bob chooses the value from a set $\{1, ..., N\}$, Alice can assign to this variable a flat distribution, i.e. $p_X(i) = 1/N$, and emulate the purified protocol to find a cheating unitary transformation as in Eq. (7.12). When it requires that the concealment is ideal, then Alice's cheating is universal for all values of Bob's secret.

However, we are normally in a non-ideal case where the concealment is permitted to be measured by $1-\epsilon$ with a negligible value of $\epsilon > 0$. Here, we say that the protocol is nearly ideal if $N\epsilon \leq \delta \ll 1$. In such a case Alice's cheating transformation is also universal with which Alice has a cheating possibility in order of $1-\delta$ for any choice of secret S. Nevertheless, when the number of possible values of S is large in order of ϵ, i.e. $N\epsilon \geq 1$, then there will be an open problem on the possibility of a non stable game on Bob's choice of the secret. The response to the question that whether such a game really exists should require further consideration.

7.4 Discussion on Irreversibility and Reversibility

The topics of reversible computation are mostly studied in relation with Landauer's principle of thermodynamical reversibility when resolving the paradox of "Maxell's demon" about whether an intelligent being could violate the second law of thermodynamics: the erasure of one bit of information in a computational device is necessarily accompanied by a generation of $kT \ln 2$ heat [Lan61, Ben82, Bub01a, Ben03].

A remarkable result from Theorem 7.2 is that, unconditionally secure oblivious transfer and bit commitment can only be made with help of a trusted third party which hides some information from Alice and Bob. Theorem 7.2 implies that we have to have a trusted third party which causes an logical erasure of information and so, similar to Maxell's Demon, generates heat, cf. Figure 7.9. It is convenient to see that the third party has limited resource, and if Alice and Bob invoke the request for many times, it begins to erase its private memory by reset all to $|0\rangle$ or to overwrite its memory and thus generate heat.

Corollary 7.2 (Irreversibility of OT and BC)**.** *Any quantum implementation unconditionally secure oblivious transfer and bit commitment requires erasure of information from the joint views of Alice and Bob, and thus causes thermodynamical reversibility and leads dissipation of heat to the environment.*

It was shown that any logically reversible computation could be thermodynamically reversible and implemented without heat dissipation, and vice versa, any thermodynamically reversible computing process must be logically reversible [Ben82, Ben00]. Moreover, it was shown that any computation could be logically reversible, by Turing machine model [Ben73] or by logic circuit models [Tof80, FT82].

This result is intuitively conformed to the impossibility of implementation of oblivious transfer and bit commitment, as the all of two-party protocols are logically invertible:

- In a classical protocol, Alice and Bob can do any local computation reversibly [Ben73], for instance by using universal reversible gates instead of normal irreversible gates AND, OR, ... [Tof80, FT82]. Therefore, the joint computation is a reversible process over all variables at Alice and Bob locations.

- In a quantum protocol, we expect that measurements will achieve some erasure of information. However, Alice and Bob can keep all of computations at the quantum level *without measurement* even the final measurements because in an ideal protocol, the users should learn the results with certainty.

Then in the end of the protocols, Alice and Bob can make a copy of the results, and undo all of the operations to reestablish the thermodynamical condition. So the impossibility of such a non-erasing protocol for oblivious transfer and bit commitment is intuitive.

Of course, when the users deny this behavior by throwing private information then the erasure appears and we have an oblivious transfer protocol. For instance, the private measurements for making Alice's and Bob's private classical variables could lead to a logical erasure of information, and therefore we can implement oblivious transfer by forcing Bob to measure the quantum signals [Cré94, Yao95].

Obviously, it is not that the erasure of information is sufficient for implementing secure computations. As analyzed in Section 7.1.2, the measurements for making classical messages can be logically seen as unnecessarily copying some information to the external environment. In real protocols, we make lot of unnecessary amplification of information to the environment and cause unnecessary dissipation of heat.

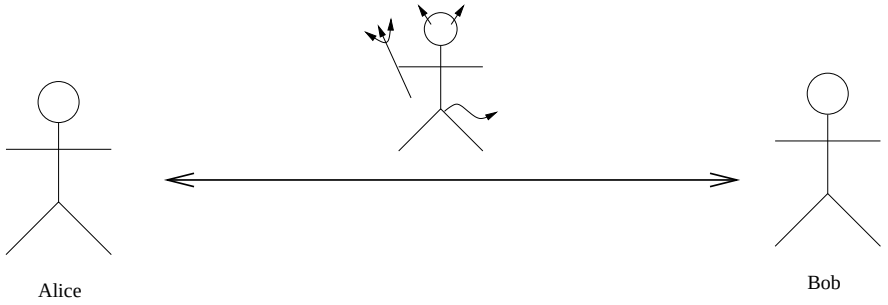

Figure 7.9: Secure two-party computations must be logically information-erasing?

A question is that: Are processes implementing unconditionally secure oblivious transfer and bit commitment *logically irreversible*?

An intuitive response from Corollary 7.2 is Yes. There are many positive symptoms for this answer. For instance, in a general two-party quantum protocol with classical communication, the global process is then *logically reversible, though physically irreversible* as Alice and Bob cannot control the external environment and then cannot implement bit commitment and oblivious transfer. Implicitly, Rabin's oblivious transfer is equivalent to a logical erasure channel. Thus, any logical process that emulates Rabin OT would require the logical erasure of information. And oblivious transfer may not be implemented by any logically reversible computing process in the joint view of Alice and Bob.

However, it's interesting to analyze the two-party oracle based protocols.

For protocol using quantum oracles, the response comes immediately from Corollary 7.2. We see that quantum two-party oracle based protocols for oblivious transfer and bit commitment required some entangled information, hidden or erased from the views of Alice and Bob.

We realize surprisingly that we can build a classical oracle for oblivious transfer, and so bit commitment, can be made with unitary transitions. Indeed, the oracle implementing oblivious transfer can be made with a unitary one:

$$\{b_0, b_1\}_A\{c, x\}_B \rightarrow \{b_0, b_1\}_1\{c, x \oplus b_c\}_B$$

where x is an auxiliary input for Bob to store the received bit. This transition is one-to-one and so there exists a reverse transition for it. Suppose that Alice and Bob send the inputs to the oracle, get the outputs, make a copy of the result, and send the outputs to an other oracle with the reverse transition which would reestablish the thermodynamical condition for the first oracle. So, could Alice and Bob realize oblivious transfer and bit commitment for

free, i.e. without dissipation of heat, by this way? Could classical world beats the quantum one in this thermodynamical battle?

The response'd rather be no, because the ultimate laws of macroscopic behaviors are governed by quantum theory. Here, we must assume that the classical oracle receives classical signals and treat them by a unitary transformation. In other words, the classical oracle is necessarily classical, acting in the classical world, not quantum superposition one.

However, a process is necessarily classical only if it is collapsed to the actual state of the environment. From this *quantum view*, a logical *necessarily* classical bit is necessarily a binary state entangled with and amplified by the environment. As in our Case-Study, cf. Section 7.2.3, a classical oracle can be build from a quantum one if it observes by measuring the signals. This observation leads some information to be stored somewhere in the memory of the oracle, and must be therefore erased as in the quantum oracle.

7.5 Concluding Remarks

In summary, we have proposed a detailed interpretation of general quantum two-party protocols where the execution is seen as a deterministic unitary evolution of a pure state covering all quantum systems including Alice's and Bob's quantum dices purifying random variables and local measurements, and environment's dices when a macroscopic channel is used for transmitting classical information.

Thus, the global state is a pure three-party state, not two-party state, where the environment's dices are not controllable by neither Alice nor Bob. However, this impurity does not help to secure bit commitment and oblivious transfer protocols. Indeed, the three-party state is in the form

$$|\Psi\rangle_{ABE*} = \sum_{i=1}^{N} \sqrt{p_b(i)}\, |i\rangle_{E*} |i\rangle_A |i\rangle_B |\psi_i\rangle_{AB}$$

Therefore, the environment does not hide information from Bob in a bit commitment protocol, and from Alice in an oblivious transfer protocol. The state can be then seen as a two-party one where $E*$ is given to the observer, while the other part can be fully controlled by the cheater.

Obviously, secure two-party computations' primitives can be trivially built with help of a trusted third-party, considered as two-party oracles. However, we have shown that the no-go theorems can also be applied to protocols that use trusted quantum oracles that compute any two-party function for Alice and Bob but splits and redirects all output quantum states to Alice and Bob, either without measurement at all or with public measurements i.e. the measurements outcomes are known by Alice and Bob. Nevertheless, coin flipping belongs to this class of trivial oracles. These works implied that two-party oracles for implementing unconditionally secure computations are required to hide or erase information and considered as dissipation of heat.

Once more, we have to be satisfied by the fact that the implementation of two-party secure computation's primitives can only be made with either conditional security that is based on assumptions on the limitation of the computing model [DFSS05, KKNY05, LMF06], or

with assumptions about trusted third-parties such as fair noisy communication media [Cré97, CMW04].

Chapter 8

Conclusion

In this thesis, we have investigated the construction of oblivious transfer, the central primitive of secure two-party computations, in the frameworks of noisy models and quantum mechanical models.

The first part of the thesis is inspired by the framework developed by Crepeau, Morozove *et al.* for building oblivious transfer as erasure models from noisy channels. We have made a contribution to this framework with the introduction of Binary Symmetric Multi-Error-Rate Channel which is a general erasure model intermediating between noisy channels and oblivious transfer. Indeed, we can exploit a gap between a set of small error rates, as *good* set, and a set of greater error rates, as *bad* set, of the BSMERC to efficiently build oblivious transfer. This extended approach helps to make use of the probability distibution of error rates for gaining a more efficient construction of oblvious transfer than the existing ones based only on the gap between the minimal error rate as the best, and the other greater error rates.

Moreover, we can go further to consider the construction of BSMERC from DMC: what input pair x_1, x_2 of the DMC should be used for implementing oblvious transfer with optimal efficiency? Here, x_1, x_2 would be selected for *good* distribution of error rates of the BSMERC and for efficient verification of Alice honesty via statistical test [Mor05].

However, this approach to such improvement of efficiency is ad-hoc and depends on the probability distribution of error rates, cf. Chapter 5. An open problem is left for further consideration of the optimal construction of oblivious transfer protocol from the BSMERC. We are motivated to do further researches on the efficiency optimization in this framework. Besides, we expect that, the consideration of this general intermediate model will be extended to continuous error-rate set BSMERC and then to general noisy continuous alphabet channels. It also requires further works to be investigated for quantitative analysis of implementation of oblivious transfer from these continuous channels.

Relatedly to this framework of noisy models, we proposed a case-study on a quantum nonorthogonal coding with two orthogonal pure quantum states, in comparison with the largely exploited quantum conjugate coding. We exposed that the QNOC can be used to emulate the desired noisy model. In each of such emulation scheme, we analyzed the application of quantum coherent measurements for optimal parameters for the receiver. These

analyses emphasize the precaution of quantum coherent attack for security parameters in protocol-reduction schemes which combine existing protocols as subroutines to build others protocols. We should consider the security parameters of composite protocol under quantum coherent attacks which are realized on the global quantum system on adversary side. However, the quantum coding is unfair because the sender can change the parameters of the emulated noisy models. We could so implement only weak oblivious transfer with non-ideal parameters. Nevertheless, while proposing a mechanism for forcing Alice to behave as semi-honest, based on coin flipping and bit commitment subroutines, we presented also how a quantum attack using two-party entanglement could be seen as quantum semi-honest but not classically semi-honest. Thus, our proposal for coin-flipping based protocol is flawed and the one for bit-commitment based protocol is secure.

The second part of this thesis is inspired by the no-go theorems of building quantum oblivious transfer and bit commitment protocols, issued by Mayers and Lo-Chau [May97, LC97, Lo97]. We proposed a reinterpretation of the quantum model for two-party protocols, clarifying the problems of private classical variables and the communication of classical information via a macroscopic channel. We exposed that the general model is indeed a three-party system consisting of Alice's machine, Bob's machine and the environment systems coupled to the classical channel. This protocol configuration is no more a pure two-party quantum state to which the theorems referred. However, the theorems remain valid on this model. With this faithful interpretation, we could extend the theorems to oracle based protocols with some constraint features of the oracles to be used. We pointed out that if the quantum oracles do not erase information then they cannot help to build quantum oblivious transfer and bit commitment protocols. Thus, coin flipping cannot be used to build oblivious transfer or bit commitment protocol.

With these generalizations, we state that, with two-party coins $\sqrt{1/2}(|0_A0_B\rangle+|1_A1_B\rangle)$ and many-party coins $\sqrt{1/2}(|0_A0_B0_{...}\rangle+|1_A1_B1_{...}\rangle)$, unconditionally secure two-party bit commitment and oblivious transfer remain impossible. Nevertheless, we can do many interesting tasks with these coins: establishing secret key [BB84], reducing communication cost [BW92], teleporting unknown quantum state [BBC$^+$93], sharing secrets [HBB99], anonymously transmitting information [CW05], ...

Moreover, we could assert that unconditionally secure oblivious transfer is by definition an information-erasing process which can only be implemented with help of a trusted third party with erasure of information, for instance noisy channels [Cré97, CMW04]. This result implied a dissipation of heat to the environment in implementations of unconditionally secure two-party computations. Nevertheless, a classical protocol based on an oracle can be logically reversible, and thus thermodynamically reversible [Ben73]. This absurdity suggested that we have to reconsider what are necessarily classical information and computation. An information is necessarily classical only if it is entangled with and amplified by the environment, and thus implicitly requires to be erased.

After all, this thesis has been primarily concerned with the *physics of information and computation*, a new inspiring discipline for computer scientists and physicists.

> "Information, after all, is something that is encoded in the state of a physical system; a computation is something that can be carried out on an actual physically

realizable device. So the study of information and computation should be linked to the study of the underlying physical processes." [Pre]

The formalism of computational processes in the physical framework becomes less abstract than the classical one such as Turing machine. Indeed, any computation is a transition from an initial state to a final state of a physical system, cf. Figure 3.1 on page 37. This could help us to remove the assumption about the computing model based on Turing's abstract machine. This physical-like formalism makes thus a firmer foundation for computer science.

Particularly, when the physical devices' diameters attain the atomic scale, their behaviors should be quantum mechanical. The works at this interface of quantum physics and information is promotive for both information processing and communication. It lets open doors into fruitful new disciplines of Algorithmics, Computational Complexity, Comunication Complexity, Information Theory, ... that would welcome an motivated reseachers.

Bibliography

[AvDK+04] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science - FOCS'04*, pages 42–51, 2004.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179. IEEE Press, 1984.

[BBB+92] C. H. Bennett, F. Bessette, G. Bassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3 – 28, 1992.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[BBCM95] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915 – 1923, 1995.

[BBCS92] C. H. Bennett, G. Brassard, C. Crépeau, and M. H. Skubiszewska. Practical quantum oblivious transfer. In *Proceedings of Advances in Cryptology - CRYPTO'91*, volume 576, pages 362 – 371, 1992.

[BCJL93] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, pages 362 – 371, 1993.

[BCMS97] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail. A brief review on the impossibility of quantum bit commitment, 1997, quant-ph/9712023.

[BCvD] H. Buhrman, R. Cleve, and W. van Dam. Quantum entanglement and communication complexity. *SIAM Journal on Computing*, 30:1829 – 1841.

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824 – 3851, 1996, quant-ph/9604024.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964.

[Ben73] C. H. Bennett. Logical reversibility of computation. *IBM Journal of Research and Development*, 17:525 – 532, 1973.

[Ben82] C. H. Bennett. The thermodynamics of computation? a review. *International Journal of Theoretical Physics*, 21:905 – 940, 1982.

[Ben92] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992.

[Ben00] C. H. Bennett. Notes on the history of reversible computation. *IBM Journal of Research and Development*, 44:270 – 277, 2000.

[Ben03] C. H. Bennett. Notes on Landauer's principle, reversible computation, and Maxwell's demon. *Studies in the History and Philosophy of Modern Physics*, 34:501 – 510, 2003.

[BF05] G. Brassard and C. A. Fuchs. Quantum foundations in the light of quantum cryptography, 2005. Invited talk at Quantum Physics of Nature & 6th European QIPC Workshop, Vienna, Austria.

[BMS96] C. H. Bennett, T. Mor, and J. A. Smolin. The parity bit in quantum cryptography. *Phys. Rev. A*, 54:2675–2684, 1996, quant-ph/9604040.

[BS98] C. H. Bennett and P. W. Shor. Quantum information theory. *IEEE Transactions on Information Theory*, 44(6):2724 – 2742, 1998.

[Bub01a] J. Bub. Maxell's demon and the thermodynamics of computation. *Studies in the History and Philosophy of Modern Physics*, 32:569 – 579, 2001, quant-ph/0203017.

[Bub01b] J. Bub. The quantum bit commitment theorem. *Foundations of Physics*, 31(5):735–756, 2001, quant-ph/0007090.

[Bus97] P. Busch. Is the quantum state (an) observable? In *Potentiality, Entanglement and Passion-At-A-Distance: Quantum Mechanical Studies for Abner Shimony*, page 61. Kluwer Academic Pub, 1997, quant-ph/9604014.

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one-and-two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69(20):2881–2884, 1992.

[CBH03] R. Clifton, J. Bub, and H. Halvorson. Characterizing quantum theory in terms of information-theoretic constraints. *Foundations of Physics*, 33:1561–1591, 2003, quant-ph/0211089.

[Che03] C.-Y. Cheung. Quantum bit commitment can be unconditionally secure, 2003, quant-ph/0112120v3.

[Che05] C.-Y. Cheung. Secret parameters in quantum bit commitment. In *Proceedings of ERATO Conference on Quantum Information Science - EQIS'05 (Poster)*, 2005, quant-ph/0508180.

[Che06] C.-Y. Cheung. Insecurity of quantum bit commitment with secret parameters, 2006, quant-ph/0601206.

[CK88] C. Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions. In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 42 – 52, 1988.

[CMW04] C. Crépeau, K. Morozov, and S. Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In *Proceedings of Fourth Conference on Security in Communication Networks - SCN'04*, pages 47–59, 2004.

[Cré88] C. Crépeau. Equivalence between two flavours of oblivious transfers. In *Proceedings of Advances in Cryptography - Crypto'87*, volume 293, pages 350 – 354, 1988.

[Cré89] C. Crépeau. Verifiable disclosure of secrets and applications. In *Proceedings of Advances in Cryptology - EUROCRYPT'89*, pages 181 – 191, 1989.

[Cré90] C. Crépeau. *Correct and Private Reductions among Oblivious Transfers*. PhD thesis, Massachusetts Institute of Technology, 1990.

[Cré94] C. Crépeau. Quantum oblivious transfer. *Journal of Modern Physics*, 41(12):2445 – 2454, 1994.

[Cré97] C. Crépeau. Efficient cryptographic protocols based on noisy channels. In *Proceedings of Advances in Cryptology - EUROCRYPT'97*, pages 306–317, 1997.

[CT91] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley, 1991.

[CW77] J. L. Carter and M. N. Wegman. Universal classes of hash functions. In *Proceedings of the 9th Annual ACM Symposium on Theory of Computing - STOC'77*, pages 106–112, 1977.

[CW05] M. Christandl and S. Wehner. Quantum anonymous transmissions. In *Proceedings of Advances in Cryptology - ASIACRYPT'05*, pages 217–235, 2005, quant-ph/0409201.

[Dan06] M.-D. Dang. More extensions of weak oblivious transfer. In Marc Bui, editor, *Proceedings of IEEE International Conference on Computer Science, RIVF - RIVF'06*, pages 40 – 44, Ho Chi Minh City, Vietnam, 2006.

[Dan07] M.-D. Dang. Improving unconditional oblivious transfer from noisy channels. In *Proceedings of The 6th WSEAS International Conference on Information Security and Privacy (ISP'07)*, pages 1 – 9, Tenerife, Spain, 2007.

[Deu] D. Deutsch. Lectures on quantum computation at the Center of Quantum Computation, University of Oxford. *Videos available at* http://cam.qubit.org/video_lectures/lectures.php.

[DFSS05] I. B. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science - FOCS'05*, pages 449–458, 2005, quant-ph/0508222.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22:644 – 654, 1976.

[Die88] D. Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 126:303–307, 1988.

[DKS99] I. B. Damgard, J. Kilian, and L. Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumtions. In *Proceedings of Advances in Cryptology - EUROCRYPT'99*, pages 56–73, 1999.

[dKSW06] G. M. d'Ariano, D. Kretschmann, D. Schlingmann, and R. F. Werner. Quantum bit commitment revisited: the possible and the impossible, 2006, quant-ph/0605224.

[dW02] R. de Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1, Natural computing):337 – 353, 2002.

[EGL85] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637 – 647, 1985.

[Eke91] A. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661 – 663, 1991.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777 – 780, 1935.

[FGGS00] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution. Technical report, MIT, 2000.

[FT82] E. Fredkin and T. Toffoli. Conservative logic. *International Journal of Theoretical Physics*, 21:219 – 253, 1982.

[Fuc95] C. A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory.* PhD thesis, University of New Mexico, USA, 1995, quant-ph/9601020.

[FvdG99] C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216 – 1227, 1999, quant-ph/9712042.

[GL00] D. Gottesman and H.-K. Lo. From quantum cheating to quantum security. *Physics Today*, 53(11):22, 2000, quant-ph/0111100.

[Gol01] O. Goldreich. *Foundations of Cryptography - Volume I: Basic Tools*. Cambridge University Press, 2001.

[Gol04] O. Goldreich. *Foundations of Cryptography - Volume II: Basic Applications*. Cambridge University Press, 2004.

[Gri04] D. J. Griffiths. *Introduction to Quantum Mechanics*. Prentice Hall, 2rd edition, 2004.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th annual ACM Symposium on Theory of computing - STOC'96*, pages 212 – 219, 1996.

[HBB99] M. Hillery, V. Buzek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59(3):1829–1834, 1999, quant-ph/9806063.

[HJW93] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Phys. Rev. A*, 183:14–18, 1993.

[HMU01] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, 2001.

[Iva87] I. D. Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 123:257–259, 1987.

[JAW+00] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71:1675–1680, 2000.

[Joz94] R. Jozsa. Fidelity for mixed quantum states. *J. Mod. Opt.*, 41:2315 – 2323, 1994.

[JS95] G. Jaeger and A. Shimony. Optimal distinction between two non orthogonal quantum states. *Physics Letters A*, 197:83–87, 1995.

[Ken99] A. Kent. Coin tossing is strictly weaker than bit commitment. *Phys. Rev. Lett.*, 83:5382, 1999, quant-ph/9810067.

[Ker83] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, 9:5 – 83, 1883.

[Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 20 – 31, 1988.

[Kit02] A. Kitaev. Quantum coin-flipping. *Talk at QIP 2003*. Slides and videos available at http://www.msri.org/publications/ln/msri/2002/qip/kitaev/1/index.html, 2002.

[KKNY05] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In *Proceedings of Advances in Cryptology - EUROCRYPT'05*, pages 268–284, 2005.

[KM01] V. Korjik and K. Morozov. Generalized oblivious transfer protocols based on noisy channels. In *Proceedings of the International Workshop on Information Assurance in Computer Networks - MMM-ACNS '01*, pages 219–229, London, UK, 2001. Springer-Verlag.

[Kre95] I. Kremer. Quantum communication. Master's thesis, Computer Science Department, The Hebrew University of Jerusalem, 1995.

[Lan61] R. Landauer. Dissipation and heat generation in the computing process. *IBM Journal of Research and Development*, 5:183 – 191, 1961.

[LC97] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible ? *Phys. Rev. Lett.*, 78:3410 – 3413, 1997.

[LC98] H. K. Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D.*, 120:177–187, 1998, quant-ph/9711065.

[LC99] H. K. Lo and H. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999, quant-ph/9803006.

[LMF06] X. Lu, Z. Ma, and D.-G. Feng. A computationally secure quantum oblivious transfer scheme. In *The 8th International Conference in Advanced Communication Technology - ICACT 2006*, volume 3, pages 1547– 1551, 2006.

[Lo97] H. K. Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154 – 1162, 1997, quant-ph/9611031.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39:733, 1993.

[May96] D. Mayers. The trouble with quantum bit commitment, 1996, quant-ph/0603015.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414 – 3417, 1997.

[Mor05] K. Morozov. *On cryptographic primitives based on noisy channels*. PhD thesis, Department of Computer Science, University of Aarhus, Denmark, 2005.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[NC04] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2004.

[Nie03] M. A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state. *Phys. Lett. A*, 308:96–100, 2003.

[Per88] A. Peres. How to differentiate between non-orthogonal states. *Physics Letters A*, 128:19, 1988.

[Per02] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 2002.

[PQC06] *International Workshop on Post-Quantum Cryptography - PQCrypto 2006*, 2006.

[Pre] J. Preskill. Lecture notes of caltech course on quantum information and quantum computation. *Available at* http://www.theory.caltech.edu/-people/preskill/ph229/.

[Rab81] M. O. Rabin. How to exchange secrets by oblivious transfer. *Technical report TR-81, Aiken Computation Laboratory, Harvard University*, 1981.

[RB01] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188 – 5191, 2001.

[Rol04] J. Roland. *Adiabatic Quantum Computation*. PhD thesis, Universite Libre de Bruxelles, 2004.

[Sch04] M. Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Rev. Mod. Phys.*, 76:1267–1305, 2004, quant-ph/0312059.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28-4:656–715, 1949.

[Sho94] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484 – 1509, 1994.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441 – 444, 2000, quant-ph/0003004.

[Sti95] D. R. Stinson. *Cryptography - Theory and Practice*. CRC Press, 1995.

[SvD00] A. M. Steane and W. van Dam. Physicists triumph at "guess my number". *Physics Today*, 53:35–39, 2000.

[SW02] D. Stebila and S. Wolf. Efficient oblivious transfer from any non-trivial binary-symmetric channel. In *Proceedings of 2002 IEEE International Symposium on Information Theory - ISIT'02*, page 293, 2002.

[TBZG98] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of Bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.*, 81:3563 – 3566, 1998, quant-ph/9806043.

[Tof80] T. Toffoli. Reversible computing. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, pages 632 – 644, 1980. adapted and condensed version of MIT Technical Report MIT/LCS/TM-151.

[vDMV01] W. van Dam, M. Mosca, and U. Vazirani. How powerful is adiabatic quantum computation? In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science - FOCS'01*, pages 279– 287, 2001.

[Wat99] J. Watrous. PSPACE has constant-round quantum interactive proof systems. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science - FOCS'99*, pages 112–119, 1999.

[Wie83] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1):78 – 88, 1983. original manuscript written circa 1970.

[Wyn75] Aaron D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54:1355–1387, 1975.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802 – 803, 1982.

[Yao86] A. C.-C. Yao. How to generate and exchange secrets. In *Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science*, pages 162 – 167, 1986.

[Yao95] A. C.-C. Yao. Security of quantum protocols against coherent measurements. In *Proceedings of the 27th Annual ACM Symposium on Theory of Computing - STOC'95*, pages 67–75, 1995.

[Yue97] H. P. Yuen. Quantum information theory, the entropy bound, and mathematical rigor in physics. In O. Hirota, A. S. Holevo, and C. M. Caves, editors, *Quantum Communication, Computing, and Measurement*, pages 17–23. Plenum Press, Newyork, 1997.

[Yue00] H. P. Yuen. Unconditionally secure quantum bit commitment is possible, 2000, quant-ph/0006109, v7.

[Yue02] H. P. Yuen. Quantum bit commitment and unconditional security, 2002, quant-ph/0207089v3.

[Yue04] H. P. Yuen. How to build unconditionally secure quantum bit commitment protocols, 2004, quant-ph/0305144v3.

[Zur91] W. H. Zurek. Decohenrence and the transition from quantum to classical. *Physics Today*, 44:36–44, 1991, quant-ph/0306072.