Université de Montréal

Hypothèses calculatoires en cryptographie quantique

par

Paul Dumais

Département d'Informatique et recherche opérationnelle

Faculté des arts et des sciences

Thèse présentée à la Faculté des études supérieures
en vue de l'obtention du grade de Philosophiæ Doctor (Ph.D.)
en Informatique

Juillet 2002

Université de Montréal

Faculté des études supérieures

Cette thèse intitulée:

Hypothèses calculatoires en cryptographie quantique

présentée par:

Paul Dumais

a été évaluée par un jury composé des personnes suivantes:

Gilles Brassard
président-rapporteur

Claude Crépeau
directeur de recherche

Alain Tapp
membre du jury

Richard E. Cleve
examinateur externe

Claude Leroy
représentant du doyen de la FÉS

Résumé

Outre la communication secrète, la cryptographie moderne s'intéresse aux protocoles permettant à deux parties qui ne se font pas confiance d'effectuer un calcul commun sur des données secrètes à chacune. Afin d'établir la sécurité d'un protocole, on doit généralement faire la démonstration que tout comportement dangereux de la part d'une des parties est théoriquement équivalent à l'accomplissement d'une tâche considérée infaisable. La plupart des protocoles en usage aujourd'hui sont basés sur l'hypothèse qu'il est infaisable de factoriser de grands nombres entiers. L'avènement de l'ordinateur quantique pourrait bouleverser ces idées reçues car un algorithme quantique pour factoriser des grands nombres existe déjà sur papier. De plus, un théorème d'impossibilité interdit tout espoir d'implanter avec sécurité inconditionnelle, même dans le modèle quantique, la *mise en gage de bit*, une primitive cryptographique fondamentale. La cryptographie bipartite vit désormais sous la menace d'un hypothétique ordinateur quantique.

Nous nous intéressons donc aux conséquences théoriques sur la cryptographie de la prise en compte du paradigme du calcul quantique, en particulier à la possibilité de fonder les primitives de *mise en gage de bit* et de *transfert inconscient* sur des hypothèses calculatoires quantiques. Nous montrons que ces deux primitives peuvent être construites sous l'hypothèse que des *permutations à sens unique* quantiques existent. Dans le cas du *transfert inconscient*, la preuve de sécurité est partielle.

Mots clés: informatique quantique, primitive cryptographique, bipartite, réduction, protocole, permutation à sens unique, mise en gage, transfert inconscient.

Summary

The *bit commitment* primitive is a key ingredient in two party cryptography where both participants want to compute a public function of their private inputs. Since the discovery of the impossibility theorem stating that unconditionally secure quantum bit commitment cannot exists, quantum cryptography in the two party case must rely on assumptions. We are considering quantum computational assumptions. Those assumptions have to be different from their classical cousins since *factoring large integers*, a computational assumption widely in use nowadays, is under attack by a quantum algorithm.

We are interested in the possibility of basing the *bit commitment* and *oblivious transfer* cryptographic primitives on quantum computational assumptions. We show that those two primitives can be constructed if we assume that quantum *one-way permutations* exist. In the case of *oblivious transfer*, the security proof is incomplete.

Key words: quantum cryptography, computational assumption, quantum computing, cryptographic primitive, bipartite, reduction, protocol, one-way permutation, bit commitment, oblivious transfer.

Table des matières

Table des figures

Remerciements

Mes premiers remerciements s'adressent à mon directeur de recherche, Claude Crépeau, qui m'a accordé son entière confiance dès le début de cette aventure. Sans son indéfectible soutien scientifique, moral et financier, ce travail n'aurait jamais vu le jour. Il y a cinq ans, le jour où je l'ai rencontré pour une première fois, il m'a dit: "Je suis partant!" Maintenant, ça y est: nous arrivons à bon port.

Je ne saurais passer sous silence l'immense contribution de mon collègue et ami Louis Salvail. Les principes sous-jacents aux preuves du chapitre 5 ont été élaborés avec lui lors de ces nombreuses conversations, que ce soit de vive voix ou par téléphone à travers l'Atlantique. Son intuition de *cryptographe quantique* est l'une des plus pénétrantes qu'il m'ait été donné d'apprécier.

Je remercie mes proches, parents et amis, pour leur soutien moral, en particulier ma mère, Thérèse, dont la patience a été mise à rude épreuve, mais qui n'a jamais perdu la foi, ne serait-ce qu'une seconde, j'en suis sûr.

Je salue mes collègues de bureau, Hugo Touchette, Geneviève Arboit et Simon-Pierre Desrosiers, qui ont fait preuve d'un tact inouï à ces multiples occasions où ils ont eu à priser mon humour.

Je remercie le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), le Fonds pour la Formation de chercheurs et l'aide à la recherche du Québec (FCAR), et la Faculté des études supérieures de l'Université de Montréal (FÉS) pour leur soutien financier.

Chapitre 1

Introduction

1.1 La cryptographie à la croisée des chemins

Depuis des siècles, la tâche dévolue à la cryptographie a été d'assurer la confidentialité des messages secrets. Le début de l'histoire des chiffres, des cryptographes et des cryptanalystes est généralement associé à l'époque de Jules César. Un chiffre fameux qui porte son nom consistait à remplacer chaque lettre d'un message par la lettre qui la suit d'un certain nombre fixé de positions dans l'alphabet. Le reste de l'aventure est bien connue: un cryptanalyste trouve une faille dans le système, un cryptographe trouve un chiffre plus robuste, et ainsi de suite. La plus grande partie de l'ouvrage classique de Kahn sur l'histoire de la cryptographie, *The Code Breakers* [Kah96], est consacrée à cette quête du système inviolable et aux efforts surhumains déployés afin de *craquer* chaque tentative.

C'est au début des années 80 que la physique quantique frappe à la porte de la cryptographie [BBE92] avec le protocole de distribution de clef [Wie83, BB84]. Par une conversation publique authentifiée et grâce à l'utilisation d'un canal quantique, ce protocole permet à deux parties de générer et partager une clef secrète.

Non seulement ce système semble incarner le Saint-Graal de la cryptographie, mais il est à la portée de la technologie actuelle [BBB+92]. Doit-on en conclure que le métier de cryptographe sera bientôt caduc?

La disparition de la cryptographie n'est pas pour demain. D'une part, il y a loin de la coupe aux lèvres. La découverte du protocole quantique de distribution de clef a généré un vaste mouvement de recherche multidisciplinaire — informatique, physique et ingénierie — en vue de sa réalisation concrète et un grand volume de publications en a découlé. D'autre part, la physique quantique n'a pas apporté que des bonnes nouvelles à la cryptographie. Les principes théoriques qui sont à la base du protocole de distribution de clef permettent également la conception de ce qu'il convient d'appeler l'*ordinateur quantique*. Le nouveau paradigme de l'informatique quantique pose de nouvelles questions et surtout lance de nouveaux défis théoriques à la cryptographie.

On ne peut pas tout faire avec le protocole de distribution de clef. Depuis la publication de *New Directions in Cryptography* par Diffie et Hellman en 1976 [DH76], date à laquelle on fixe le début de la cryptographie moderne, les cryptographes ne se contentent plus de chiffrer les messages secrets. Ils ont développé des systèmes cryptographiques *à clef publique* qui permettent à deux parties de communiquer secrètement même s'ils ne partagent pas une clef secrète commune [DH76], une théorie de l'authentification [Sim92b], des systèmes de signature numérique [DH76, Mer79], les calculs multipartites sécurisés [GMW87] et les preuves interactives *zero-knowledge* [GMR89]. Du scénario classique où deux parties tentent de s'échanger un message secret à l'abri du regard indiscret d'un tiers, la science cryptographique s'intéresse maintenant à des situations plus élaborées, à plusieurs parties, parmi lesquelles certaines peuvent être corrompues. La sécurité de beaucoup des protocoles que nous venons de mentionner repose sur la complexité calculatoire présumée de certaines tâches et non pas sur le fait que des participants partagent une clef secrète. Nous dirons alors que la sécurité repose sur une *hypo-*

thèse calculatoire.

Une des pierres angulaires de l'édifice cryptographique moderne est sérieusement ébranlée par l'algorithme quantique de Shor [Sho97]. Si l'ordinateur quantique voit le jour, on pourra, grâce à cet algorithme, calculer en temps raisonnable les facteurs de grands nombres entiers, une tâche considérée infaisable sur un ordinateur classique. De nos jours, la sécurité de nombreux systèmes cryptographiques repose sur l'hypothèse que la factorisation ne peut être réalisée qu'à un coût prohibitif en temps de calcul. L'algorithme de Shor existe déjà sur papier et s'il devient réalité, la cryptographie retourne à l'âge de pierre. Il est donc vital de s'intéresser dès aujourd'hui aux tâches cryptographiques dont la sécurité devra un jour ou l'autre reposer sur une hypothèse calculatoire quantique.

1.2 Modèles symétrique et asymétrique en cryptographie quantique

Nous nous intéressons dans cette thèse aux protocoles cryptographiques quantiques bipartites. Nous l'avons déjà mentionné, le champ de la cryptographie moderne est beaucoup plus vaste, mais nous verrons que ce domaine où nous nous restreignons est déjà riche et les problèmes à résoudre y sont nombreux, subtils et non triviaux. Afin de bien cerner le terrain sur lequel nous nous aventurons, le tableau synoptique apparaissant à la figure 1.1[4] tiendra lieu de guide.

Les deux colonnes de ce tableau illustrent les deux types de scénarios bipartites auxquels la cryptographie quantique s'intéresse. Annonçons d'ores et déjà que notre sujet d'étude se rattache à la deuxième colonne, que nous avons baptisée *le modèle asymétrique* par opposition au scénario symétrique du protocole de distribution de clef.

Le modèle symétrique	Le modèle asymétrique
Les deux parties se font confiance.	Les deux parties se méfient l'une de l'autre.
L'adversaire est un tiers.	L'adversaire joue le rôle d'une des deux parties.
La primitive fondamentale est la *distribution de clef.*	Les primitives fondamentales sont la *mise en gage* et le *transfert inconscient.*
Des conditions de sécurité inconditionnelle sont réalisables pour les deux parties.	Une hypothèse calculatoire est nécessaire pour au moins l'une des deux parties.
Les preuves de sécurité reposent sur la théorie de l'information pour les deux parties.	Les preuves de sécurité reposent sur la théorie de la complexité du calcul pour l'une des deux parties.

FIG. 1.1 – *Cryptographie quantique à deux parties*

Notons au passage que l'expression *cryptographie quantique* est utilisée dans notre texte avec un sens plus large qu'il ne lui est généralement attribué dans la littérature. En effet, les termes *cryptographie quantique* (*quantum cryptography* en anglais) sont souvent pris pour synonymes de *distribution quantique de clef* (*QKD, quantum key distribution*), alors que nous y englobons la mise en gage quantique (*quantum bit commitment*) et le transfert inconscient quantique (*quantum oblivious transfer*), les deux primitives fondamentales du modèle asymétrique.

Reprenons un à un chacun des éléments du tableau 1.1[4]. La première ligne fait ressortir la différence fondamentale entre les deux modèles. Dans le modèle asymétrique, les deux parties — baptisons-les maintenant Alice et Bob, comme le veut la tradition — ne se font pas confiance, mais chacun participera volontiers au protocole, pourvu qu'un minimum de sécurité soit garanti dans le cas où le vis-à-vis serait malhonnête. L'exemple le plus simple de tâche illustrant cette situation est sans doute le *tir à pile ou face*, où Alice et Bob désirent obtenir un bit, `0` ou `1`, choisi uniformément au hasard. Le tir à pile ou face est nécessaire dans de nombreux protocoles cryptographiques et il est clair que la sécurité d'un protocole est compromise si Alice ou Bob est en mesure de biaiser la valeur des bits aléatoires. Mentionnons les protocoles d'identification et les calculs bipartites sécurisés (Alice et Bob désirent calculer une fonction publique sur des données privées) parmi les scénarios asymétriques.

Concernant la deuxième ligne du tableau, il est nécessaire de préciser que, dans le modèle asymétrique, *nous ne considérons jamais le cas où Alice et Bob sont simultanément malhonnêtes*. La cryptographie existe pour protéger les gens honnêtes, et si plus personne n'est honnête, alors le problème de sécurité ne se pose plus.

Aux primitives fondamentales de *mise en gage* et *de transfert inconscient*, mentionnées à la troisième ligne du tableau dont nous reparlerons à la section 1.3[6], nous aurions pu ajouter le *tir à pile ou face*. Nous ne l'avons pas fait parce que cette primitive peut être facilement réalisée à partir d'une mise en gage [Blu82]. Remarquons que les articles traitant du tir à pile ou face comme primitive cryptographique quantique, notamment [Amb01], abordent la question du point de vue de la sécurité inconditionnelle, et non pas en fondant la tâche sur une hypothèse calculatoire, ce qui sera notre approche dans ce travail. C'est sur la mise en gage de bit que l'on peut en partie fonder les preuves [GMR89] et les arguments [BCC88] *zero-knowledge* et le transfert inconscient est une primitive universelle pour le calcul bipartite sécurisé [Kil88a].

Enfin les deux dernières lignes de notre tableau décrivent l'essence de l'approche que nous avons choisie. Alors que le protocole de distribution de clef a été démontré inconditionnellement robuste face à une grande famille d'attaques [May96], un théorème d'impossibilité nous interdit tout espoir de construire une mise en gage inconditionnellement sécuritaire pour les deux parties [LC97, May97]. Il est nécessaire de noter qu'à une certaine époque on a cru à la sécurité inconditionnelle

nelle d'un certain protocole implantant la primitive de mise en gage [BCJL93], ce qui aurait conféré à la cryptographie quantique une aura d'invulnérabilité tant dans le modèle asymétrique que le dans modèle symétrique. Il appert, par le théorème d'impossibilité déjà mentionné, que ce ne soit pas le cas, ce qui rend somme toute le domaine plus intéressant. Il est donc nécessaire de s'en remettre à une hypothèse calculatoire comme cela est d'usage en cryptographie classique. Mais notre hypothèse sera *quantique*, c'est-à-dire qu'elle s'inscrira dans le modèle calculatoire quantique. Notre *permutation à sens unique* en sera une *quantique*, c'est-à-dire qu'elle sera facilement calculable et difficilement inversable *sur un ordinateur quantique*. Cette hypothèse n'est nécessaire que pour garantir la sécurité d'une seule des deux parties, car, nous le rappelons, une seule partie est considérée malhonnête dans l'analyse d'un scénario bipartite asymétrique.

Dans la prochaine section, nous cernons davantage le sujet de cette thèse, et adoptons définitivement le point de vue de la dépendance entre les diverses primitives cryptographiques.

1.3 Hiérarchies de primitives cryptographiques

1.3.1 Les primitives

Il est temps de définir les diverses primitives cryptographiques que nous avons déjà mentionnées et celles auxquelles nous aurons affaire un peu plus loin.

Les définitions qui suivent sont encore informelles et évitent plusieurs subtilités, mais elles seront adéquates pour cette introduction. Les termes *infaisable*, *efficace* et *significativement* sont volontairement laissés flous. Nous ne distinguons pas pour l'instant les réductions *non uniformes* des réductions *uniformes*. Nous ne faisons pas non plus la distinction entre la sécurité *parfaite* et la sécurité *statistique* qu'on trouve dans la littérature : nous utilisons le terme *inconditionnelle* pour les deux notions. Nous adoptons des acronymes anglais pour désigner chaque primitive, afin d'alléger la lecture aux habitués de la littérature existante qui est rédigée presque uniquement dans cette langue.

L'idée de mise en gage de bit est introduite par Blum dans [Blu82]. Le terme d'*oblivious transfer* [Rab81] est né avec une définition différente de ce que nous appelons dans ce texte *transfert inconscient*. Notre *transfert inconscient* correspond à *one-out-of-two oblivious transfer* dans la littérature [Wie83, EGL85]. Les concepts de fonction à sens unique et de fonction à sens unique avec brèche remontent à [DH76] et [Mer79].

BC_B et BC_H : Mise en gage (*Bit Commitment*). Alice a un bit b inconnu de Bob qu'elle veut lui transmettre, mais de façon différée. Cette tâche comporte deux phases d'interaction entre Alice et Bob: l'engagement et l'ouverture. Entre ces deux phases, Alice ne peut pas modifier la valeur de b et Bob ne peut la connaître. La valeur de b ne sera révélée à Bob que pendant la phase d'ouverture, s'il y a lieu. Cette primitive donne lieu à deux variantes qui sont duales l'une de l'autre.

- BC_B : Mise en gage inconditionnellement liante et calculatoirement camouflante (*Bit Commitment/Binding*). Aucune puissance du calcul ne permettrait à Alice de modifier la valeur de b une fois la phase d'engagement complétée; cette impossibilité est garantie par la théorie de l'information. Bob ne peut deviner la valeur du bit caché avec probabilité de succès significativement plus grande que $1/2$ que si une certaine hypothèse calculatoire est brisée, c'est-à-dire qu'une tâche considérée infaisable soit à la portée calculatoire de Bob.

- $\mathsf{BC_H}$: Mise en gage calculatoirement liante et inconditionnellement camouflante (*Bit Commitment/Hiding*). L'impossibilité pour Bob de deviner la valeur de b avec probabilité de succès significativement meilleure que $1/2$ est garantie par la théorie de l'information. Alice ne peut modifier la valeur de b que si une certaine hypothèse calculatoire est transgressée.

$\mathsf{OT_R}$ **et** $\mathsf{OT_S}$ **: Transfert inconscient (*One-out-of-two Oblivious Transfer*).** Nous baptisons provisoirement les protagonistes *Rachel* pour la réceptrice, et *Sam* pour l'envoyeur (*sender*). Sam détient deux bits a_0 et a_1 et Rachel a un bit de choix c. À la fin du protocole, Rachel obtient le bit a_c et ne connaît pas la valeur du bit non choisi et Sam ignore la valeur de c. Cette primitive est également offerte en deux saveurs selon le côté où repose la sécurité inconditionnelle.

- $\mathsf{OT_S}$: Le transfert camoufle inconditionnellement le bit de choix à Sam et camoufle calculatoirement un des deux bits à Rachel.
- $\mathsf{OT_R}$: Le transfert camoufle inconditionnellement un des deux bits à Rachel et camoufle calculatoirement le bit de choix à Sam.

OWF **: Fonction à sens unique (*One-Way Function*).** Une fonction $f \equiv \left\{f_k \ : \ \{0,1\}^k \rightarrow \{0,1\}^{\ell(k)}\right\}_{k>0}$ est à dite sens unique si elle est calculable efficacement et si la tâche de trouver une pré-image d'un élément $f(\boldsymbol{x})$ donné de l'image est difficile, lorsque $\boldsymbol{x}$ est uniformément choisi au hasard dans $\{0,1\}^k$.

OWP **: Permutation à sens unique (*One-Way Permutation*).** La fonction $\pi \equiv \left\{\pi_k \ : \ \{0,1\}^k \rightarrow \{0,1\}^k\right\}_{k>0}$ est une permutation à sens unique si π est une fonction à sens unique et si π_k, la restriction de π au domaine $\{0,1\}^k$, est une permutation pour tout k.

TOWP : Permutation à sens unique avec brèche (*Trap-door One-Way Permutation*). La permutation à sens unique π est dite *avec brèche* s'il devient possible de claculer $\pi^{-1}(y)$ efficacement pour tout $y \in \{0,1\}^k$, étant donnée une information auxiliaire qui dépend de k mais pas de y.

1.3.2 La hiérarchie classique

Les primitives ayant été présentées, nous allons maintenant donner une vue d'ensemble des réductions connues qui existent entre elles dans le monde classique. Dit informellement, il existe une réduction d'une primitive P_1 à une primitive P_2, ce qui sera noté $P_1 \leq P_2$, si on peut réaliser la primitive P_1, étant donné que P_2 est réalisable. On dira alors que P_2 est *plus forte* que P_1, ou, plus correctement, que P_2 *n'est pas plus faible* que P_1.

Évidemment, le simple énoncé $P_1 \leq P_2$ ne dit pas tout sur le prix à payer pour obtenir P_1 étant donné P_2. Combien d'appel à P_2 seront nécessaires? La réduction demande-t-elle de l'interactivité entre les deux participants et, si oui, combien de messages doivent être envoyés de part et d'autre? Quel est le coût de la réduction en temps de calcul? Et enfin, de quelle façon, exprimée par rapport à un certain paramètre de sécurité, la robustesse de de P_1 dépend-elle de la robustesse de P_2?

On répond généralement à cette dernière question en exhibant une réduction d'un adversaire à P_2 à un adversaire à P_1, ce qui peut être noté $\mathcal{A}_{P_2} \leq \mathcal{A}_{P_1}$. Autrement dit, on explicite une façon d'attaquer P_2 étant donnée une façon d'attaquer P_1. Si on croit, par exemple, que P_2 est innattaquable, nous serons forcés de croire que P_1 l'est également. Cette façon de faire est principalement utilisée pour démontrer la sécurité lorsqu'elle repose ultimement sur une hypothèse calculatoire, par opposition à une preuve de sécurité basée sur la théorie de l'information.

Les réductions qui mettent en scène les primitives de mise en gage ou de transfert

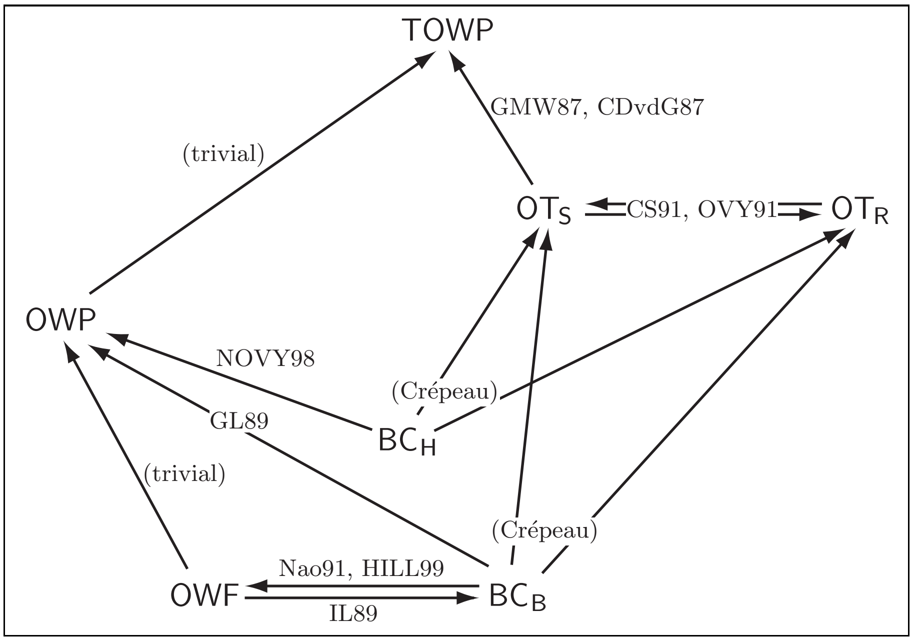


Fig. 1.2 – *Hiérarchie de primitives en cryptographie: le monde classique*

inconscient comportent deux côtés, un pour chacune des deux parties. La sécurité par rapport à la malhonnêteté d'un des participants sera garantie de façon inconditionnelle et l'autre côté sera calculatoirement sécurisé. Par abus de langage, nous décrirons cette situation en parlant du *côté calculatoire* et du *côté inconditionnel* de la réduction.

La hiérarchie apparaît à la figure 1.2[10]. Nous ne prétendons pas que ce schéma soit exhaustif, mais il nourrit certainement notre intuition sur la force relative de chaque primitive. De plus, cette hiérarchie est un nécessaire préambule à son pendant quantique qui sera présentée à la section 1.3.3[12]. Une flèche d'une primitive P_1 vers une primitive P_2 indique qu'on connaît une réduction de P_1 à P_2. Les primitives les plus fortes se retrouvent vers le haut du diagramme. Les références appropriées apparaissent le long des flèches et des remarques dans les paragraphes qui suivent.

$\mathsf{BC_B} \leq \mathsf{OWF}$. La réduction est réalisée indirectement par $\mathsf{BC_B} \leq \mathsf{PRBG} \leq \mathsf{OWF}$ où PRBG signifie *générateur pseudo-aléatoire cryptographique* (*Pseudo-Random Bit Generator*). Les détails peuvent être lus dans [Lub96].

$\mathsf{BC_B} \leq \mathsf{OWP}$. Cette fois, nous avons $\mathsf{BC_B} \leq \mathsf{OWPr} \leq \mathsf{OWP}$ où OWPr signifie *prédicat à sens-unique* (*One-Way Predicate*), la première des deux réductions étant triviale. Voir encore [Lub96].

$\mathsf{BC_H} \leq \mathsf{OWP}$. Notons que cette réduction demande $\Omega(k)$ ronde d'interactivité entre Alice et Bob où k est un paramètre de sécurité.

$\{\mathsf{BC_B},\mathsf{BC_H}\} \leq \{\mathsf{OT_S},\mathsf{OT_R}\}$. Ces réductions sont attribuées à Claude Crépeau dans [Kil88b], [Cré01].

$\mathsf{OT_S} \leq \mathsf{OT_R}$ et $\mathsf{OT_R} \leq \mathsf{OT_S}$. Telles que publiées, ces preuves de sécurité, de même que celles du paragraphe précédent, sont essentiellement basées sur la théorie de l'information parce que les auteurs supposent qu'ils ont à leur disposition une boîte noire implantant le transfert inconscient avec sécurité parfaite des deux côtés. Cela est une hypothèse beaucoup plus forte que ce que nous nous permettons d'utiliser. Nous insistons sur le fait qu'une telle preuve n'est pas directement applicable aux côtés calculatoires de nos réductions. Essentiellement, une preuve basée sur la théorie de l'information établit que *toute information permettant d'attaquer P_1 permet d'attaquer P_2*. Alors qu'une preuve basée sur la calculabilité se lit *toute information facilement calculable permettant d'attaquer P_1 permet d'attaquer facilement P_2*. Mais les preuves de sécurité mentionnées peuvent être adaptées afin de démontrer la sécurité des côtés calculatoires des réductions à $\mathsf{OT_S}$ ou à $\mathsf{OT_R}$ [Cré01] (en invoquant un argument *hybride* tel que celui exposé dans [Lub96] utilisé pour construire un générateur de fonctions pseudo-aléatoires depuis un générateur pseudo-aléatoire [GGM86], ou tels qu'ils sont utilisés à plusieurs reprises dans [Gol98]).

$\mathsf{OT}_\mathsf{S} \leq \mathsf{TOWP}$. Cette réduction se fait au moyen de mises en gage dont certaines doivent être construites par $\mathsf{BC}_\mathsf{H} \leq \mathsf{OWP}$ [NOVY98] afin d'assurer le côté inconditionnel.

Notons qu'on ne sait pas laquelle de BC_B ou BC_H est la plus forte ou si elles sont comparables. Par ailleurs, il est vraisemblable que le transfert inconscient soit une primitive strictement plus forte que la mise en gage et les permutations à sens unique [IR89].

1.3.3 La hiérarchie quantique

Qu'advient-il de ce diagramme si l'on tient compte du modèle calculatoire quantique? On serait porté à croire que toute réduction établie sur le modèle classique peut être directement et aveuglément transportée au monde quantique, puisqu'après tout l'ordinateur quantique est au moins aussi puissant que l'ordinateur classique. La situation est loin d'être aussi simple! Par exemple, la réduction classique $\mathsf{BC}_\mathsf{H} \leq \mathsf{OWP}$ [NOVY98] ne tient plus dans le monde quantique. Le problème vient du fait que l'analyse de la sécurité de la réduction d'un inverseur de la permutation à un adversaire à la condition liante de BC_H — ce qu'on peut noter $\mathcal{A}_\mathsf{OWP} \leq \mathcal{A}_{\mathsf{BC}_\mathsf{H}}$ — utilise un adversaire déterministe muni d'un ruban aléatoire externe et la technique de *rembobinage* (*rewinding*). Que cette technique de preuve soit généralement incompatible avec le modèle quantique [vdG97, page 112] est essentiellement dû au fait que lorsqu'une machine quantique fait un choix aléatoire, l'état dans lequel se trouvait cette machine antérieurement s'est irrémédiablement évaporé, et on ne peut à la fois tenir compte de ce choix aléatoire et rembobiner la machine à son état initial. Dans le cas de la relation $\mathsf{BC_H} \leq \mathsf{OWP}$, si la preuve de sécurité de [NOVY98] était transposée au modèle quantique en accordant à l'adversaire une forme de rembobinage quantique, alors on pourrait obtenir un algorithme quantique efficace inversant toute fonction à sens unique [vdG97, page 114], tuant dans l'oeuf la raison d'être de la réduction.

Par contraste, la réduction $\mathsf{BC_B} \leq \mathsf{OWP}$ est sécuritaire d'une façon plus probante dans le modèle quantique, parce que la réduction $\mathcal{A}_{\mathsf{OWP}} \leq \mathcal{A}_{\mathsf{BC_B}}$ peut bénéficier de la technique quantique d'amplification d'amplitude [AC01].

Finalement, les définitions mêmes des primitives et de leurs adversaires doivent être adaptées correctement aux particularités du modèle quantique, que ce soit la modélisation des adversaires à l'aide de familles de circuits ou la prise en compte de la possibilité que les entrées à une primitive telle que $\mathsf{BC_H}$ puissent exister en superposition.

Nous introduisons donc notre graphe quantique à la figure 1.3[14]. Les acronymes OWF et OWP ont été préfixés de la première lettre du mot *quantique*.

La différence marquante entre les deux graphes est que, dans le modèle quantique, la mise en gage est au moins aussi forte que le transfert inconscient. Cela est dû au protocole de Crépeau [Cré94] qui implante le transfert inconscient à l'aide de mises en gage de bits et de communication quantique. Encore une fois, la réduction de Crépeau de même que la preuve de sécurité due à Yao [Yao95] sont essentiellement basées sur la théorie de l'information. Il faut dire qu'à cette époque on croyait encore aux mises en gage quantique inconditionnellement sécuritaires des deux côtés à la fois [BCJL93, Cré96], puisque le théorème d'impossibilité n'est apparu que quelque temps plus tard [LC97, May97]. Le côté calculatoire de $\mathsf{OT_R} \leq \mathsf{BC_B}$ est fait dans [CLS01].

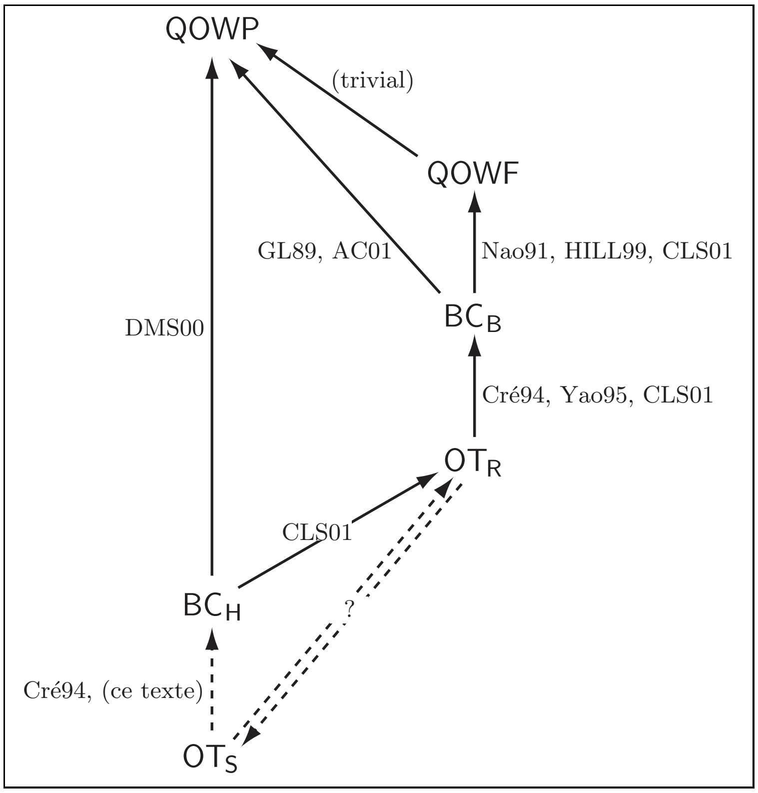


FIG. 1.3 – *Hiérarchie de primitives en cryptographie: le monde quantique*

Le côté calculatoire de $\mathsf{OT_S} \leq \mathsf{BC_H}$ est l'un des objets de cette thèse. La flèche indiquant cette réduction est mise en pointillé car la réduction $\mathcal{A}_{\mathsf{BC_H}} \leq \mathcal{A}_{\mathsf{OT_S}}$ que nous offrons ne couvre pas tous les cas d'adversaires $\mathcal{A}_{\mathsf{OT_S}}$. Autrement dit, nous offrons une preuve de sécurité qui est partielle et perfectible. Nous reviendrons à ces considérations en temps et lieu, c'est-à-dire au chapitre 5.

On remarque également qu'il existe une réduction indirecte $\mathsf{BC_H} \leq \mathsf{BC_B}$ due à [CLS01]. On ignore si une telle relation est vraie en cryptographie classique.

Il y a bon espoir qu'il soit possible de transporter au modèle quantique les réductions entre $\mathsf{OT_S}$ et $\mathsf{OT_R}$ qui apparaissaient à la figure 1.2[10] [Cré01]. Mais comme ces réductions n'ont pas encore été examinées sérieusement, nous préférons jouer de prudence et nous les indiquons au moyen de flèches pointillées à la figure 1.3[14].

1.4 Contributions de cette thèse

Le domaine de nos contributions apparaît clairement à la figure 1.3[14]. Il s'agit de l'axe $\mathsf{OT_S} \leq \mathsf{BC_H} \leq \mathsf{QOWP}$.

Le résultat $\mathsf{BC_H} \leq \mathsf{QOWP}$ [DMS00] fut le tout premier publié parmi ceux qui sont répertoriés à la figure 1.3[14] et il découle d'une initiative que l'on doit à Louis Salvail — l'auteur de cette thèse a contribué à l'élaboration des preuves, des notations et de la modélisation quantique des primitives. Non seulement cette réduction constitue-t-elle le fondement la cryptographie quantique calculatoire, mais elle vient combler un vide créé par la prise en compte même du modèle quantique. En effet, un résultat semblable existe en cryptographie classique [NOVY98], mais, nous l'avons mentionné à la section 1.3.3[12], la preuve classique ne peut être adaptée au modèle quantique. De plus, la réduction de [DMS00] est non interactive par opposition à la réduction classique qui demande $\Omega(n)$ rondes d'interaction entre

Alice et Bob, pour un paramètre de sécurité n.

La preuve de sécurité du côté calculatoire de la réduction $\mathsf{OT_S} \leq \mathsf{BC_H}$ est le fruit d'un travail en collaboration avec Louis Salvail, Claude Crépeau et Dominic Mayers. Il est important de faire ressortir la valeur de notre approche en la juxtaposant à celle de [Yao95]. La preuve de Yao n'est valide que du point de vue de la théorie de l'information. Yao présume l'existence de mises en gage inconditionnellement sécuritaires des ceux côtés à la fois — un modèle qualifié parfois par l'expression *boîte noire* — et il montre qu'un tricheur jouant le rôle du receveur dans le protocole de transfert inconscient ne détient qu'une quantité négligeable d'information à propos du bit qui doit rester secret selon les spécifications du protocole. Notre preuve, quant à elle, n'a besoin d'aucune hypothèse au sujet des mises en gage. L'adversaire $\mathcal{A}_{\mathsf{OT_S}}$ est modélisé par des circuits quantiques et ces circuits sont utilisés tels quels dans la construction d'un adversaire $\mathcal{A}_{\mathsf{BC_H}}$ à la condition liante des mises en gage. Incidemment, notre démarche est valide aussitôt qu'un adversaire à $\mathsf{OT_S}$ peut être modélisé par un calcul quantique et son champ d'application généralise — et inclut — celui de la preuve de Yao.

Le rôle du *prouveur* est ingrat si on compare sa tâche à celle de la conception d'un protocole. Le concepteur d'un protocole cryptographique met tout en oeuvre afin d'en *simplifier* les spécifications et le déroulement. Par exemple, le protocole quantique de transfert inconscient que nous étudions est suffisamment simple pour être en principe implanté au moyen de la technologie actuelle puisqu'il n'exige des participants honnêtes que la transmission de photons polarisés dans les bases canoniques ou diagonales de même que des mesures dans ces deux bases [Cré94]. Par contre, lorsqu'il s'agit de démontrer la sécurité d'un tel protocole, aucun compromis ne peut être toléré: on doit tôt ou tard considérer *tous les adversaires* possibles. Toute hypothèse émise au sujet de l'adversaire mène à une preuve de sécurité partielle, voir par exemple [MS94]. En ce qui concerne notre réduction $\mathcal{A}_{\mathsf{BC_H}} \leq \mathcal{A}_{\mathsf{OT_S}}$, nous avons également dû nous restreindre à une certaine classe d'adversaires $\mathcal{A}_{\mathsf{OT_S}}$, mais notre approche ouvre la voie à la recherche d'une réduction qui serait valide dans tous les cas. Une valeur ajoutée à une telle démonstration consisterait donc à mettre un protocole réalisable aujourd'hui à l'abri des attaques de demain, même celles qui pourraient le cas échéant être implantées à l'aide d'un ordinateur quantique.

1.5 Plan de la thèse

Nous consacrons le chapitre 2 aux notions préliminaires nécessaires à la compréhension de l'exposé. La terminologie et les principales notations, conventions et définitions y sont introduites. Quelques résultats utiles sur les mises en gage classiques sont énoncés et démontrés à la section 2.5[35]. Le chapitre 3 est consacré à la réduction $\mathsf{BC_H} \leq \mathsf{QOWP}$. Au chapitre 4, nous considérons quelques aspects techniques reliés à la sécurité d'une mise en gage quantique de plusieurs bits étant donnée une primitive permettant de s'engager à un seul bit. Ces considérations sont nécessaires au chapitre suivant. Une preuve partielle de sécurité de la réduction $\mathsf{OT_S} \leq \mathsf{BC_H}$ est présentée au chapitre 5. Nous concluons au chapitre 6 et présentons quelques avenues de recherche. Entre autres, ce dernier chapitre regroupera et synthétisera les questions non résolues — ou volontairement laissées floues — des chapitres 4 et 5.

Chapitre 2

Notions préliminaires

Ce chapitre contient les définitions, les conventions, les notations et la terminologie de base dont nous auront besoin par la suite.

2.1 Conventions et notations générales

Nous empruntons à la physique le symbole $\equiv$ pour introduire la définition d'une expression. Notons que l'expression définie peut apparaître autant du côté droit du signe $\equiv$ que du côté gauche.

On aura recours aux notions asymptotiques de comportement polynômial ou négligeable d'une fonction:

Définitions 2.1 (*polynômial et négligeable*). Une fonction d'un paramètre entier k a un comportement asymptotique (lorsque $k \to \infty$) *polynômial* si elle est bornée supérieurement par un polynôme à partir d'un certain entier k_0, et *négligeable* si elle est bornée supérieurement par tout inverse de polynôme à partir d'un certain

k_0. On peut exprimer ces notions à l'aide de la notation grand-O ensembliste, voir [Bra85]:

$$\begin{aligned} \mathrm{poly}(k) &\equiv \bigcup_{j>0} O(k^j), \\ \mathrm{negl}(k) &\equiv \bigcap_{j>0} O(\frac{1}{k^j}). \end{aligned}$$

Si le comportement est polynômial par rapport au logarithme de k, alors on note

$$\mathrm{polylog}(k) \equiv \bigcup_{j>0} O(\log^j(k)).$$

▲

La tradition définit qu'un algorithme est *efficace* si son temps d'exécution en fonction de la taille de l'input a un comportement aymptotique polynômial. Cette notion d'efficacité a l'avantage d'être robuste par rapport au modèle calculatoire adopté, pourvu qu'il soit *raisonnable* [GJ79].

Lorsqu'on considérera une famille d'objets indexés par un paramètre entier, disons n, il est possible qu'on ne puisse définir l'objet correctement pour tous les n, mais seulement pour un sous-ensemble infini des nombres entiers, par exemple tous les n pairs à partir d'un certain n_0. On convient d'emblée que la définition ou la proposition en question ne sera considérée valide que pour ces entiers-là, sans qu'on ait à expliciter cette mise en garde à chaque fois.

Nous regroupons ci-dessous les notations concernant les chaînes de bits.

Notations 2.2 (*chaînes de bits*). Les variables désignant des chaînes de bits sont notées au moyen d'une police grasse (comme $\boldsymbol{x} \in \{\mathtt{0},\mathtt{1}\}^\ell$). Le j-ème bit de la chaîne $\boldsymbol{x}$ est noté $\boldsymbol{x}[j]$. L'expression $\boldsymbol{x}[j_1,\ldots,j_2]$ désigne la sous-chaîne de longueur $j_2 - j_1 + 1$ extraite de $\boldsymbol{x}$ aux positions j_1 à j_2. La *chaîne vide* est notée par ε.

La *juxtaposition* de chaînes de bits est notée au moyen de tuplets comme $(\boldsymbol{x},\boldsymbol{y})$, ou par l'absence d'opérateur comme dans $\mathtt{01}$, ou au moyen de l'opérateur $\Diamond$:

$$\boldsymbol{x} = \bigDiamond_{j=1}^{n} \boldsymbol{x}[j].$$

Les expressions $\boldsymbol{x} \wedge \boldsymbol{y}$, $\boldsymbol{x} \vee \boldsymbol{y}$, $\boldsymbol{x} \oplus \boldsymbol{y}$ et $\bar{\boldsymbol{x}}$ gardent leurs sens habituels: *et*, *ou*, *ou exclusif* et *négation*, respectivement. Le *produit scalaire* de deux chaînes est noté

$$\boldsymbol{x} \odot \boldsymbol{y} \equiv \bigoplus_{j} \boldsymbol{x}[j] \wedge \boldsymbol{y}[j],$$

le *bit de parité* et le *poids de Hamming*:

$$\begin{aligned} \|\boldsymbol{x}\| &\equiv \boldsymbol{x} \odot \boldsymbol{x} = \bigoplus_{j} \boldsymbol{x}[j], \\ |\boldsymbol{x}| &\equiv \sum_{j} \boldsymbol{x}[j]. \end{aligned}$$

L'expression $\boldsymbol{x} \preceq \boldsymbol{y}$ signifie que le support de $\boldsymbol{x}$ est inclus dans le support de $\boldsymbol{y}$:

$$\boldsymbol{x} \preceq \boldsymbol{y} \quad \iff \quad \forall j \ : \ \boldsymbol{x}[j] = \mathtt{1} \implies \boldsymbol{y}[j] = \mathtt{1}.$$

▲

Voici deux notations concernant les expériences aléatoires:

Notation 2.3 (*expérience aléatoire et probabilité*). L'expression

$$\{ \textit{ expérience aléatoire } \}\mathrm{Prob}[\textit{événement}]$$

désigne la probabilité d'un événement conditionné à une certaine expérience aléatoire, généralement écrite en pseudo-code. ▲

Notation 2.4 (*choix aléatoire uniforme*). L'expression $x \stackrel{\mathcal{U}}{\leftarrow} E$ signifie que x est choisi aléatoirement et uniformément parmi les élément de l'ensemble E. ▲

2.2 Loi des grands nombres

Nous insérons ici une version utile de la *loi des grands nombres*, qui a le don d'ubiquité en cryptographie. La version générale de cette loi est due à Hoeffding [Hoe63]. La loi affirme que la probabilité que le nombre de succès, lors de n expériences indépendantes, s'éloigne de la moyenne par une quantité proportionnelle à n est négligeable en n.

Proposition 2.5 (*loi des grands nombres*). Soient $X_1, \ldots, X_n \in \{0,1\}$ n variables aléatoires indépendantes et identiquement distribuées suivant une loi de Bernoulli de paramètre p, c'est-à-dire

$$\forall i \in \{1,\ldots,n\} \ : \ \mathrm{Prob}[X_i = 1] = p \text{ et } \mathrm{Prob}[X_i = 0] = 1 - p,$$

et soit $\delta > 0$. Alors

$$\mathrm{Prob}\left[\sum_{i=1}^{n} X_i - pn \geq \delta n\right] \ \leq \ e^{-2\delta^2 n} \in \mathrm{negl}(n)$$

et

$$\mathrm{Prob}\left[\sum_{i=1}^{n} X_i - pn \leq -\delta n\right] \ \leq \ e^{-2\delta^2 n} \in \mathrm{negl}(n).$$

▲

2.3 Calcul quantique

Le but de cette section n'est pas d'offrir un cours d'introduction détaillé au calcul quantique. D'excellentes introductions au domaine existent déjà et nous encourageons le lecteur à les consulter [NC00, Bra99, Ber97], ou [CTDL73] pour la physique quantique. Nous allons donc présumer connues la terminologie et les notions de base de l'informatique quantique et de l'algèbre linéaire. Nous tenons cependant à donner certaines définitions ou notations qui pourraient s'éloigner de l'usage le plus courant.

2.3.1 Conventions et notations générales pour le calcul quantique

Le calcul quantique fait un copieux usage de l'algèbre linéaire. Nous utiliserons indifféremment les termes *transformation linéaire* ou *opérateur linéaire*, ou plus simplement *transformation* ou *opérateur*. Nous abrégeons également *mesure de von Neumann* par *mesure.*

Il va s'en dire que tous les opérateurs et états quantiques que nous manipulons sont de dimension finie et qu'ils sont construits sur le corps des nombres complexes. Comme nous travaillons en dimension finie, il est permis d'assimiler un opérateur ou un état quantique à sa représentation matricielle dans la base canonique, ce que nous ferons sans aucune gêne. Cette base est parfois appelée *base calculatoire*, *base de calcul* ou *base rectilinéaire.* Les physiciens diraient *la base dans laquelle l'opérateur de changement de phase conditionnel σ_z est diagonal.* Les éléments de la base canonique $\mathcal{B}$ d'un espace de dimension d sont identifiés au moyen des entiers de 0 à $d-1$ ou à la représentation binaire de ces entiers lorsque la dimension est une puissance de 2, $d = 2^\ell$:

$$\mathcal{B} \;=\; \{\, |j\rangle \,\}_{0 \leq j < d} \;=\; \{\, |\boldsymbol{x}\rangle \,\}_{\boldsymbol{x} \in \{0,1\}^\ell} \;.$$

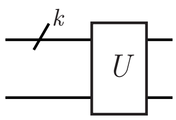
Nous réservons la police *tableau noir* (comme $\mathbb{P}$, $\mathbb{M}$) aux projecteurs et aux mesures. Les états quantiques sont généralement désignés par des lettres grecques (comme $|\psi\rangle$, ρ).

Notation 2.6 (*vecteurs et états normalisés*). Les *kets* (comme $|\psi\rangle$) désignent des vecteurs de norme 1, et on prendra soin de noter au moyen d'une flèche (comme $\vec{\lambda}$) les vecteurs qui ne sont pas nécessairement normalisés. ▲

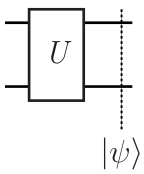
2.3.2 Conventions graphiques pour les circuits quantiques

Dans les diagrammes illustrant des circuits quantiques, l'information circule de gauche à droite, comme d'habitude. On retranscrit généralement de gauche à droite les registres figurant de haut en bas sur un diagramme. Si une ambiguïté subsiste, alors les noms des registres seront indiqués en exposant à l'opérateur ou état (comme $|\psi\rangle^{\text{Alice,Charles}} \otimes |\phi\rangle^{\text{Bob}}$). S'il est fastidieux d'énumérer tous les registres, on utilisera le nom de registre fourre-tout *Etc* (comme $|\psi\rangle^{\text{Etc}} \otimes |\phi\rangle^{\text{Bob}}$). Le signe $\otimes$ sera omis là où il n'y a aucun danger de confondre produit tensoriel et produit ordinaire d'opérateurs, et des parenthèses seront ajoutées là où il y a danger de confondre la préséance de ces deux opérations.

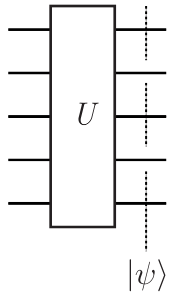
La taille des registres de plus d'un qubit est indiquée au moyen d'un trait oblique dans les diagrammes. Par exemple,



désigne un registre de k qubits au-dessus d'un registre de 1 qubit. Un trait oblique sans légende indique un registre d'un nombre non spécifié de qubits, pas nécessairement 1. L'état des registres à une étape du calcul est indiqué à l'aide d'une barre verticale pointillée: le schéma



montre que les registres sont dans l'état $|\psi\rangle$ à la sortie de la porte U. Si on veut indiquer que seulement une partie des registres sont dans un certain état, alors on pourra oblitérer la barre verticale:

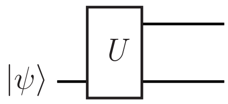


montre qu'à la sortie de la porte U les premier, troisième et cinquième registres peuvent être factorisés et ils sont conjointement dans l'état $|\psi\rangle$.

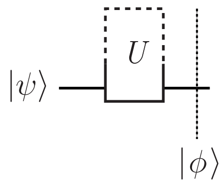
Il arrive que l'on veuille considérer l'état initial de certains registres à l'entrée d'un circuit comme fixé à une valeur convenue. Nous utiliserons alors la notation suivante:

Notation 2.7 (*état initial pour les circuits*). On note par $|\vdash\rangle$ le vecteur $|0\rangle$ de la base canonique, quelle que soit la dimension de l'espace considéré. ▲

Dans les diagrammes, cet état initial est indiqué par l'*absence* du registre au départ d'un circuit. Par exemple, la porte U ci-dessous



prend l'état $|\vdash\rangle|\psi\rangle$ en entrée. Si on veut également ignorer l'état du registre en sortie, on utilisera la convention suivante:



signifie que $U : |\vdash\rangle|\psi\rangle \mapsto |\phi\rangle$, la taille du registre ancillaire demeurant non spécifiée. Cette notation permet d'indiquer la présence d'un registre de travail pour

U, et de supposer sans perte de généralité que U est unitaire, sans toutefois polluer le diagramme avec des registres dont on veut faire abstraction. S'il n'y a pas de risque d'ambiguïté, les états $|\vdash\rangle$ et les transformations $\mathbb{1}$, de même que les étiquettes des registres, peuvent être omis à la retranscription:

$$(U^{\mathrm{A}} \otimes \mathbb{1}^{\mathrm{B,C}})(|\vdash\rangle^{\mathrm{A,B}}|\psi\rangle^{\mathrm{C}}) \quad\equiv\quad U^{\mathrm{A}}|\psi\rangle^{\mathrm{C}} \quad\equiv\quad U|\psi\rangle.$$

2.3.3 Transformations unitaires

Les transformations unitaires suivantes sont d'usage courant.

Notations 2.8 (*transformations unitaires usuelles*). La transformation identité est notée par $\mathbb{1}$, quelle que soit sa dimension; si on tient à préciser la dimension d, elle sera indiquée en indice: $\mathbb{1}_d$. De plus, on note la transformation de Walsh-Hadamard et les opérateurs de Pauli de la façon suivante, pour tout $b \in \{\mathsf{0},\mathsf{1}\}$:

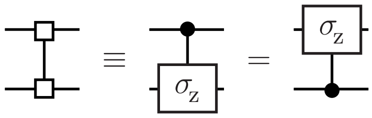
$$\begin{aligned} \mathsf{H} \quad &: \quad |b\rangle \longmapsto \sum_{x\in\{\mathsf{0},\mathsf{1}\}} (-1)^{b\wedge x}|x\rangle, \\ \mathsf{NOT} = \sigma_x \quad &: \quad |b\rangle \longmapsto |\bar{b}\rangle, \\ \sigma_y \quad &: \quad |b\rangle \longmapsto (-1)^b \mathrm{i}|\bar{b}\rangle, \\ \sigma_z \quad &: \quad |b\rangle \longmapsto (-1)^b|b\rangle. \end{aligned}$$

Une transformation U contrôlée est notée C-U. Pour un angle θ quelconque, on a la transformation de changement conditionnel de phase:

$$\mathsf{P}_\theta \quad : \quad \begin{cases} |\mathsf{0}\rangle \longmapsto |\mathsf{0}\rangle \\ |\mathsf{1}\rangle \longmapsto \mathrm{e}^{\mathrm{i}\theta}|\mathsf{1}\rangle. \end{cases}$$

▲

Graphiquement, les transformations C-NOT et C-U en général sont notées selon l'usage répandu. Cependant la transformation C-σ_z fait l'objet d'une notation graphique spéciale qui honore sa symétrie:



.

Notations 2.9 (*exponentiation tensorielle*). Si U est une transformation unitaire, si $n > 0$ est un entier et si $\boldsymbol{x} \in \{\mathtt{0},\mathtt{1}\}^n$ alors

$$U^{\otimes n} \equiv \bigotimes_{j=1}^{n} U$$

$$\text{et} \qquad U^{\otimes \boldsymbol{x}} \equiv \bigotimes_{j=1}^{n} U^{\boldsymbol{x}[j]}$$

où $U^0 = \mathbb{1}$ et $U^1 = U$. ▲

2.3.4 Bases canonique et diagonale

Comme c'est souvent le cas en cryptographie quantique, nous travaillons sans cesse avec les bases canonique et diagonale. Nous leur attribuons les notations suivantes.

Notations 2.10 (*bases canonique et diagonale*). Les expressions $|\mathtt{0}\rangle_+$, $|\mathtt{1}\rangle_+$ d'une part, et $|\mathtt{0}\rangle_\times$, $|\mathtt{1}\rangle_\times$ d'autre part désignent les éléments des bases canonique et *diagonale* respectivement. C'est-à-dire:

$$|\mathtt{0}\rangle_+ = \frac{1}{\sqrt{2}}\left(|\mathtt{0}\rangle_\times + |\mathtt{1}\rangle_\times\right), \tag{2.1}$$

$$|\mathtt{1}\rangle_+ = \frac{1}{\sqrt{2}}\left(|\mathtt{0}\rangle_\times - |\mathtt{1}\rangle_\times\right), \tag{2.2}$$

$$|\mathtt{0}\rangle_\times = \frac{1}{\sqrt{2}}\left(|\mathtt{0}\rangle_+ + |\mathtt{1}\rangle_+\right), \tag{2.3}$$

$$|\mathtt{1}\rangle_\times = \frac{1}{\sqrt{2}}\left(|\mathtt{0}\rangle_+ - |\mathtt{1}\rangle_+\right). \tag{2.4}$$

Pour $\boldsymbol{b} \in \{0,1\}^n$ et $\boldsymbol{\theta} \in \{+,\times\}^n$ on note

$$\begin{aligned}
|\boldsymbol{b}\rangle_{\boldsymbol{\theta}} &\equiv \bigotimes_{j=1}^{n} |\boldsymbol{b}[j]\rangle_{\boldsymbol{\theta}[j]}, \qquad (2.5)\\
|\boldsymbol{b}\rangle_{+} &\equiv \bigotimes_{j=1}^{n} |\boldsymbol{b}[j]\rangle_{+},\\
|\boldsymbol{b}\rangle_{\times} &\equiv \bigotimes_{j=1}^{n} |\boldsymbol{b}[j]\rangle_{\times}.
\end{aligned}$$

▲

Les équations (2.1[26]) à (2.4[26]) seront généralisées au lemme 2.30[41]. De plus, on s'accorde sur un encodage binaire désignant les deux bases:

Notation 2.11 (*encodage des bases canonique et diagonale*). Partout où un bit (`0` ou `1`) figure mais où une base ($+$ ou $\times$) devrait apparaître on identifie les symboles $+$ et `0` d'une part, et $\times$ avec `1` d'autre part. ▲

2.3.5 Projecteurs et mesures

La mesure est l'interface entre l'état quantique et l'information classique qu'on peut en tirer. Nous adoptons le formalisme des projecteurs.

Notations et définitions 2.12 (*projecteur et mesure*). Un *projecteur* $\mathbb{P}$ est un opérateur linéaire tel que $\mathbb{P}^\dagger = \mathbb{P}$ et $\mathbb{P}^2 = \mathbb{P}$, c'est-à-dire $\mathbb{P}$ est hermitien et idempotent. Une *mesure* $\mathbb{M}$ est une famille finie de projecteurs orthogonaux deux à deux et dont la somme est l'identité, ce qui sera noté

$$\mathbb{M} = [\mathbb{M}_1,\mathbb{M}_2,\ldots,\mathbb{M}_m],$$

$$\sum_{j=1}^{m} \mathbb{M}_j = \mathbb{1},$$

$$\forall j,j' \text{ tels que } j \neq j' \ : \ \mathbb{M}_j \mathbb{M}_{j'} = 0.$$

L'ensemble des indices $\{1,2,\ldots,m\}$ est l'*espace des résultats possibles* de l'expérience aléatoire qui consiste à mesurer un état quantique quelconque au moyen de la mesure $\mathbb{M}$. Lorsqu'un état pur $|\psi\rangle$ est mesuré par $\mathbb{M}$, la *probabilité de l'événement* j est donnée par

$$\begin{aligned} \{\ x \xleftarrow{\mathbb{M}} |\psi\rangle\ \}\mathrm{Prob}[x=j] &\equiv \||\mathbb{M}_j|\psi\rangle\|^2 \\ &= \langle\psi|\mathbb{M}_j|\psi\rangle \end{aligned} \tag{2.6}$$

lorsqu'un état mixte ρ est mesuré au moyen de $\mathbb{M}$, la *probabilité de l'événement* j est donnée par

$$\{\ x \xleftarrow{\mathbb{M}} \rho\ \}\mathrm{Prob}[x=j] \equiv \mathrm{tr}(\mathbb{M}_j\rho). \tag{2.7}$$

▲

Il est facile de vérifier que l'équation (2.6[28]) est bien un cas particulier de l'équation (2.7[28]) et que ces deux lignes définissent bien une distribution sur l'ensemble des résultats possibles. Une valeur propre d'un projecteur $\mathbb{P}$ vaut nécessairement 0 ou 1. Le nombre de 1 apparaissant dans la diagonalisation de $\mathbb{P}$ est le *rang* du projecteur $\mathbb{P}$. Pour un état normalisé $|\psi\rangle$, $|\psi\rangle\langle\psi|$ est un projecteur de rang 1 qui projette sa victime *le long de* $|\psi\rangle$. L'identité est un projecteur trivial de rang égal à sa dimension. Il est également facile de démontrer que la somme des rangs des projecteurs d'une mesure égale la dimension de l'espace sur lequel ces opérateurs agissent, que la somme de deux projecteurs orthogonaux est un projecteur, et que l'identité moins un projecteur donne un projecteur.

Nous n'utiliserons pas la terminologie suivante chère aux phycisiens:

Remarque 2.13 (*observable*). En reprenant les notations de la définition 2.12[27], la matrice hermitienne $\sum_{1\leq j\leq m} a_j\mathbb{M}_j$, où les a_j sont des nombres réels distincts, est un *observable* correspondant à la mesure $\mathbb{M}$. Les nombres a_j correspondent aux quantités physiques mesurées par une implantation de $\mathbb{M}$. ▲

Définition 2.14 (*mesure complète ou partielle*). Une mesure est dite *complète* si tous ses projecteurs sont de rang 1; la mesure est *partielle* dans le cas contraire. ▲

Sur le modèle de la ligne (2.5^{27}), on note:

Notations 2.15 (*mesures dans les bases canonique et diagonale*). Soit $\boldsymbol{\theta} \in \{+,\times\}^n$, alors

$$\mathbb{M}_{\boldsymbol{\theta}} \equiv \bigotimes_{j=1}^{n} \mathbb{M}_{\boldsymbol{\theta}[j]},$$

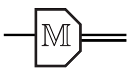
où

$$\mathbb{M}_{+} \equiv [\ |0\rangle\langle 0|,\ |1\rangle\langle 1|\ ],$$

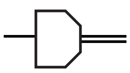
$$\mathbb{M}_{\times} \equiv [\ |0\rangle_{\times}\langle 0|,\ |1\rangle_{\times}\langle 1|\ ].$$

▲

Graphiquement, une mesure est indiquée par une porte hexagonale:



le trait double à la sortie de la porte nous rappelle que c'est l'information classique, fruit de l'observation, qui circule maintenant sur ce registre. Une forme vide



désigne une mesure complète dans la base canonique.

2.3.6 Fidélité

La fidélité est une mesure de proximité entre deux états. Si on mesure un état $|\psi\rangle$ dans une base contenant $|\phi\rangle$, alors la fidélité entre ces deux états purs est égale à la probabilité d'observer $|\phi\rangle$ lors de cette mesure. Plus généralement:

Notation et définition 2.16 (*fidélité*). Soient ρ_1 et ρ_2 deux états quelconques, alors

$$\mathcal{F}(\rho_1,\rho_2) \equiv \left(\mathrm{tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right)^2 .$$

▲

En particulier, si l'un des deux états est pur alors $\mathcal{F}(|\phi\rangle,\rho) = \langle\phi|\rho|\phi\rangle$, et si les deux états sont purs alors on aura $\mathcal{F}(|\phi\rangle,|\psi\rangle) = |\langle\phi|\psi\rangle|^2$. Il est important de signaler que certains auteurs, notamment [NC00], définissent leur *fidélité* comme la racine carrée de la nôtre.

2.3.7 Propriétés utiles en calcul quantique

Nous rappelons en vrac quelques propriétés élémentaires du calcul quantique.

La proposition suivante nous donne une généralisation tensorielle du fait qu'une combinaison linéraire nulle de vecteurs linéairement indépendants doit être triviale. Cette propriété joue un rôle dans la preuve du lemme 2.31[43].

Proposition 2.17 (*somme nulle de matrices linéairement indépendantes*). Soit $\{V_1,V_2,\ldots,V_m\}$ un ensemble de matrices de mêmes dimensions et linéairement indépendantes. On a:

$$\sum_{j=1}^{m} A_j \otimes V_j = 0 \iff \forall j : A_j = 0$$

pour peu que les matrices A_j aient les dimensions appropriées. ▲

Nous allons fréquemment faire abstraction de la présence d'un registre ancillaire de travail de taille indéterminée dans les circuits quantiques à venir. Si on mesure un état, il est important de s'assurer que la présence ou l'absence de ce registre ancillaire dans les calculs ne peut en rien influencer la distribution de probabilités sur les résultats possibles de la mesure. La proposition suivante rend compte de ce fait.

Proposition 2.18 (*probabilité associée à un projecteur local*). Soit $|\psi\rangle^{\mathrm{A,B}}$ un état bipartite. Soit $\mathbb{P}^{\mathrm{B}}$ un projecteur agissant dans l'espace $\mathcal{H}^{\mathrm{B}}$. Soit ρ^{B} la trace partielle de $|\psi\rangle^{\mathrm{A,B}}$ dans l'espace $\mathcal{H}^{\mathrm{B}}$. Alors la probabilité de l'événement associé au projecteur $\mathbb{1}^{\mathrm{A}} \otimes \mathbb{P}^{\mathrm{B}}$ sur $|\psi\rangle^{\mathrm{A,B}}$ est égale à la probabilité de l'événement associé au projecteur $\mathbb{P}^{\mathrm{B}}$ sur ρ^{B}:

$$||(\mathbb{1}^{\mathrm{A}} \otimes \mathbb{P}^{\mathrm{B}})|\psi\rangle||^2 \;=\; \mathrm{tr}(\;\mathbb{P}^{\mathrm{B}}\mathrm{tr}_{\mathrm{A}}(|\psi\rangle\langle\psi|)\;).$$

▲

De plus, un projecteur ne peut hausser une probabilité:

Proposition 2.19 (*probabilité associée à un vecteur projeté*). Soit $\mathbb{P}$ un projecteur et $\vec{v}$ un vecteur, alors

$$||\mathbb{P}\vec{v}||^2 \;\leq\; ||\vec{v}||^2.$$

▲

Dans le même ordre d'idées, la proposition suivante stipule que la probabilité associée à un projecteur, étant donnée une préparation quantique quelconque, est bornée inférieurement par la probabilité associée à un vecteur propre du projecteur.

Proposition 2.20 (*probabilité associée à un vecteur propre d'un projecteur*). Soit ρ un état quelconque, soit $\mathbb{P}$ un projecteur, et soit $|\psi\rangle$ tel que $||\mathbb{P}|\psi\rangle||^2 = 1$, alors

$$\mathrm{tr}(\mathbb{P}\rho) \geq \langle\psi|\rho|\psi\rangle.$$

▲

La fidélité de deux états ne peut qu'augmenter si un espace est ignoré:

Proposition 2.21 (*fidélité locale*). Soient $\rho_1^{\mathrm{A,B}}$ et $\rho_2^{\mathrm{A,B}}$ deux états bipartites, et soient

$$\sigma_1^{\mathrm{A}} \equiv \mathrm{tr}_{\mathrm{B}}(\rho_1^{\mathrm{A,B}}), \quad \sigma_2^{\mathrm{A}} \equiv \mathrm{tr}_{\mathrm{B}}(\rho_2^{\mathrm{A,B}}),$$

alors

$$\mathcal{F}(\sigma_1,\sigma_2) \geq \mathcal{F}(\rho_1,\rho_2).$$

▲

Voici une version d'un théorème familier formulée à l'aide de projecteurs.

Proposition 2.22 (*théorème de Pythagore*). Soient $\{\mathbb{P}_1,\mathbb{P}_2,\ldots,\mathbb{P}_m\}$ une famille de projecteurs orthogonaux deux à deux et $\{\vec{v}_1,\vec{v}_2,\ldots,\vec{v}_m\}$ des vecteurs quelconques, alors

$$\|\sum_{j=1}^{m} \mathbb{P}_j \vec{v}_j\|^2 \ = \ \sum_{j=1}^{m} \|\mathbb{P}_j \vec{v}_j\|^2.$$

▲

La proposition suivante relie la fidélité de deux états purs à la norme de la différence vectorielle entre ces deux états.

Proposition 2.23 (*fidélité et erreur*). Soient $|\psi_1\rangle$ et $|\psi_2\rangle$ deux états purs, et soit $\vec{f} \equiv |\psi_2\rangle - |\psi_1\rangle$. Alors

$$|\langle\psi_1|\psi_2\rangle|^2 \geq (1 - \frac{\|\vec{f}\|^2}{2})^2.$$

▲

Notons que dans un espace euclidien, c'est-à-dire à scalaires dans $\mathbb{R}$, l'inégalité de la proposition 2.23[32] devient une égalité.

2.4 Modèle calculatoire et réductions

Nous rappelons quelques faits élémentaires à propos du modèle usuel de calcul quantique: les circuits quantiques; voir [Cle99] pour une excellente introduction à la théorie de la complexité quantique.

À l'instar du modèle des circuits classiques, nous devons d'abord convenir d'un ensemble d'un petit nombre de portes à partir desquelles tous nos circuits seront construits. On appelle un tel ensemble un *ensemble universel* si tout ce qui est calculable peut être calculé au moyen de ces portes. Cependant, comme l'espace des états quantiques est continu et comme l'espace des circuits que l'on peut construire à partir d'un ensemble fini de portes est dénombrable, on doit se contenter d'un ensemble universel qui permet d'évaluer tout état au moyen d'une *approximation*. La proposition suivante résume cette situation [NC00, chapitre 4]:

Proposition 2.24 (*universalité d'un ensemble de portes quantiques*). Toute transformation unitaire U agissant sur un nombre quelconque de qubits peut être approchée à distance arbitrairement petite par un circuit quantique construit avec des portes choisies uniquement dans l'ensemble $\{\mathsf{H}, \mathsf{P}_{\frac{\pi}{2}}, \mathsf{P}_{\frac{\pi}{4}}, \mathsf{C\text{-}NOT}\}$, où la distance entre deux transformations unitaires U et V est donnée par

$$||U - V|| = \sup_{||\vec{\alpha}||=1} ||(U - V)\vec{\alpha}||.$$

▲

Pour des raisons pratiques, nous ajoutons quelques portes utiles à cet ensemble:

Définitions 2.25 (*ensemble universel et portes élémentaires*). L'ensemble

$$\mathcal{U} = \{\mathsf{H}, \mathsf{P}_{\frac{\pi}{2}}, \mathsf{P}_{\frac{\pi}{4}}, \mathsf{C\text{-}NOT}, \sigma_x, \sigma_z, \mathsf{C\text{-}H}, \mathsf{C}\text{-}\sigma_z\}$$

sera notre *ensemble universel* de portes quantiques. Les éléments de $\mathcal{U}$ sont des *portes élémentaires*. Pour un circuit quantique C construit à partir de $\mathcal{U}$, $||C||_{\mathcal{U}}$ désigne le nombre de portes élémentaires dans C. ▲

C'est donc la taille $\|C_k\|_{\mathcal{U}}$ d'une famille de circuits $C = \{C_k\}_{k>0}$ qui sera notre mesure de complexité, où k est le nombre de qubits en entrée au circuit C_k. Par abus de langage, ou par lapsus volontaire, nous dirons que $\|C_k\|_{\mathcal{U}}$ est le *temps* requis pour exécuter le circuit C_k. On sous-entend également le mot *uniforme* dans l'expression *C est une famille de circuits*: c'est-à-dire qu'il existe une machine de Turing (classique) qui produit une description du circuit C_k lorsqu'on lui donne 1^k en entrée. Il va s'en dire que le modèle doit permettre, en plus de l'utilisation des portes élémentaires, la préparation de l'état initial $|\vdash\rangle$ et l'exécution d'une mesure dans la base canonique. On considère que ces deux dernières opérations se font en temps $O(k)$.

Jusqu'à maintenant, nous avons délibérément omis de faire la distinction entre *réduction uniforme* et *réduction non uniforme*. Il est temps de mettre les points sur les *i*. Une réduction de la primitive P_1 à la primitive P_2 sera notée $P_1 \leq P_2$ si elle est *uniforme*, c'est-à-dire si elle est constructive: étant donné un circuit qui implante P_2, nous construisons un circuit pour P_1, en faisant bien sûr appel au circuit de P_1 comme s'il s'agissait d'une boîte noire ou d'une sous-routine mise à notre disposition. D'autre part, une réduction est *non uniforme* si elle est existentielle, et elle sera notée par $\leq_\exists$. Cela se produira surtout pour les réductions entre adversaires. Par exemple, lorsqu'on s'intéresse à la sécurité d'une réduction $P_1 \leq P_2$, l'énoncé $\mathcal{A}_{P_2} \leq_\exists \mathcal{A}_{P_1}$ signifie que l'on n'a démontré que l'existence d'un adversaire à P_2, étant donné un adversaire à P_1, sans pour autant avoir exhibé une construction de $\mathcal{A}_{P_2}$ à partir de $\mathcal{A}_{P_1}$. L'implication suivante est triviale:

$$\mathcal{A}_{P_2} \leq \mathcal{A}_{P_1} \Longrightarrow \mathcal{A}_{P_2} \leq_\exists \mathcal{A}_{P_1},$$

et le premier énoncé est donc plus fort que le second.

2.5 Mise en gage classique

Il est utile de faire le point sur la mise en gage de bit d'un point de vue strictement classique, avant de la relever au contexte quantique au chapitre 3. Nous donnons donc les détails formels définissant cette primitive telle qu'on la conçoit généralement en cryptographie classique.

2.5.1 Les définitions folkloriques

Les définitions qui suivent traduisent de façon formelle la notion de mise en gage que les cryptographes utilisent intuitivement et spontanément dans leurs conversations de corridor. La littérature, quant à elle, offre une multitude de définitions, toutes équivalentes espère-t-on, et nous avons préféré en ajouter une à la liste plutôt que de nous en remettre à un auteur particulier. Nous pouvons ainsi adapter plus facilement notre définition aux besoins de l'exposé. On trouvera les approches les plus rigoureuses dans [Lub96, Gol98].

La primitive de mise en gage est définie par deux algorithmes probabilistes, C pour la phase d'*engagement* (*commitment* en anglais) et O pour l'*ouverture*. Nous nous restreignons volontairement aux mises en gage non interactives et parfaitement camouflantes: d'une part cela simplifie la présentation et d'autre part nous n'aurons pas besoin d'étudier une primitive plus générale puisque nous réalisons une telle mise en gage par un protocole quantique à la section 3.4[54]. La *non interactivité* signifie qu'un seul message est transmis d'Alice vers Bob lors des phases d'engagement et d'ouverture.

Les algorithmes C et O sont de temps (probabiliste) poly(k) où k servira de paramètre de sécurité. Le format de leurs entrées et sorties s'exprime comme suit:

$$(\boldsymbol{c},\boldsymbol{d}) \quad \leftarrow \quad C(1^k,b); \tag{2.8}$$

$$b' \;\leftarrow\; O(\boldsymbol{c},\boldsymbol{d}) \tag{2.9}$$

où $b \in \{\mathtt{0},\mathtt{1}\}$ est le bit mis en gage par Alice et $b' \in \{\mathtt{0},\mathtt{1},\perp\}$ est le bit révélé à Bob. La sortie $\perp$ signifie que l'ouverture est rejetée par Bob, ce qui inclut le refus d'ouvrir de la part d'Alice. La chaîne $\boldsymbol{c}$, gage de la bonne foi d'Alice, est transmise à Bob à la phase d'engagement. La chaîne $\boldsymbol{d}$ ne sera transmise qu'à l'ouverture afin de permettre à Bob d'exécuter le test O.

On donne un sens cryptographique à la primitive en définissant les trois notions suivantes: la complétude du schème de mise en gage, la perfection du camouflage et la qualité d'un adversaire à la condition liante.

Définition 2.26 (*mise en gage non interactive: complétude*). Les algorithmes C et O définissent une *mise en gage non interactive* s'ils répondent aux spécifications des lignes (2.8[35]) et (2.9[36]) et s'ils satisfont la propriété de *complétude*:

$$\forall b \in \{\mathtt{0},\mathtt{1}\} \;:\; \{ \quad (\boldsymbol{c},\boldsymbol{d}) \leftarrow C(\mathtt{1}^k,b); \quad b' \leftarrow O(\boldsymbol{c},\boldsymbol{d}) \quad \}\mathrm{Prob}[b' = b] \;=\; 1. \tag{2.10}$$

▲

Autrement dit, une mise en gage honnête est toujours ouverte avec succès. Nous sommes conscients de perdre encore un peu de généralité à la ligne (2.10[36]), puisqu'on aurait pu permettre une probabilité d'échec négligeable (en k). Mais nous optons pour la simplicité en remarquant une fois de plus que notre construction centrale de la section 3.4[54] satisfait la ligne (2.10[36]).

Comme nos mises en gage sont parfaitement camouflantes, nous ne nous attarderons pas à définir un adversaire à la condition camouflante, mais définissons plutôt la sécurité de ce côté de façon positive.

Définition 2.27 (*mise en gage: camouflage parfait*). Le schème de la définition

2.26[36] est *parfaitement camouflant* si, pour tout $k > 0$, la distribution des chaînes $\boldsymbol{c}$ à la ligne (2.8[35]) est la même pour $b = \mathtt{0}$ ou pour $b = \mathtt{1}$. ▲

De l'autre côté, l'adversaire à la condition liante réussit sa tâche s'il peut faire ouvrir avec succès un $\mathtt{0}$ *et* un $\mathtt{1}$ avec un même message d'engagement:

Définition 2.28 (*mise en gage: adversaire à la condition liante*). Un *adversaire à la condition liante* d'une mise en gage telle que décrite à la définition 2.26[36] est un algorithme probabiliste $\widetilde{C}$ qui répond au format suivant:

$$(\widetilde{c}, d_{\mathtt{0}}, d_{\mathtt{1}}) \leftarrow \widetilde{C}(\mathtt{1}^k)$$

et sa *probabilité de succès* est donnée par

$$\begin{aligned} \delta(k) = \{ \quad & (\widetilde{c}, d_{\mathtt{0}}, d_{\mathtt{1}}) \leftarrow \widetilde{C}(\mathtt{1}^k); \\ & b_{\mathtt{0}} \leftarrow O(\widetilde{c}, d_{\mathtt{0}}); \\ & b_{\mathtt{1}} \leftarrow O(\widetilde{c}, d_{\mathtt{1}}) \quad \}\mathrm{Prob}[b_{\mathtt{0}} = \mathtt{0} \text{ et } b_{\mathtt{1}} = \mathtt{1}]. \end{aligned} \tag{2.11}$$

▲

Les définitions 2.26[36] et 2.27[36] peuvent aisément être adaptées au modèle quantique, comme nous le verrons à la section 3.3[50]. Le problème surgit plutôt avec la définition 2.28[37]. La modélisation même d'un test quantique, c'est-à-dire d'une mesure (définitions 2.12[27]), interdit de considérer la conjonction (le *et*) de deux événements distincts, comme c'est le cas à la ligne (2.11[37]). Il est donc nécessaire de reformuler la définition 2.28[37] avant de l'adapter au modèle quantique, ce qui est l'objectif de la section suivante.

2.5.2 Définition de l'adversaire à la condition liante adaptable au modèle quantique

À la lumière de la définition 2.28[37], considérons l'expérience aléatoire suivante:

$$A_{\widetilde{C}} \equiv \{ \quad (\widetilde{c}, d_0, d_1) \leftarrow \widetilde{C}(1^k); \quad b_0 \leftarrow O(\widetilde{c}, d_0); \quad b_1 \leftarrow O(\widetilde{c}, d_1) \quad \}, \tag{2.12}$$

et définissons les deux événements

$$\begin{aligned} E_0 &\equiv b_0 = 0, \\ E_1 &\equiv b_1 = 1. \end{aligned}$$

Alors la probabilité de succès (2.11[37]) peut se récrire

$$\delta(k) = \{A_{\widetilde{C}}\}\mathrm{Prob}[E_0 \text{ et } E_1].$$

Considérons maintenant la quantité

$$\delta'(k) = \max(0, \mathrm{Prob}[E_0] + \mathrm{Prob}[E_1] - 1). \tag{2.13}$$

D'une part il est facile de voir que, pour un adversaire $\widetilde{C}$ donné, $\delta'(k)$ est borné supérieurement par $\delta(k)$:

$$\begin{aligned} \delta'(k) &= \max(\mathrm{Prob}[E_0] + \mathrm{Prob}[E_1] - 1{,}0) \\ &\leq \mathrm{Prob}[E_0] + \mathrm{Prob}[E_1] - \mathrm{Prob}[E_0 \text{ ou } E_1] \\ &= \mathrm{Prob}[E_0 \text{ et } E_1] \\ &= \delta(k). \end{aligned}$$

Autrement dit, étant donné un bon adversaire au sens de (2.13[38]), ce même adversaire est aussi bon, sinon meilleur, au sens de (2.11[37]).

D'autre part, soit un adversaire $\widetilde{C}$ avec probabilité de succès $\delta(k)$ au sens de (2.11[37]). Considérons l'adversaire $\widetilde{C}'$ construit à l'aide de $\widetilde{C}$, C et O:

$$
\begin{aligned}
\widetilde{C}'(\mathtt{1}^k) \equiv \{ \quad & (\widetilde{c},d_0,d_1) \leftarrow \widetilde{C}(\mathtt{1}^k);\\
& \texttt{si}\ \ ((O(\widetilde{c},d_0) = \mathtt{0})\ \ \texttt{ou}\ \ (O(\widetilde{c},d_1) = \mathtt{1}))\ \ \texttt{alors}\\
& \quad \texttt{output}\ \ (\widetilde{c},d_0,d_1)\\
& \texttt{sinon}\\
& \quad (c,d_0) \leftarrow C(\mathtt{1}^k,\mathtt{0});\\
& \quad \texttt{output}\ \ (c,d_0,junk) \quad \}
\end{aligned}
$$

L'algorithme $\widetilde{C}'$ se comporte comme $\widetilde{C}$, sauf dans les cas où $\widetilde{C}$ ne peut faire ouvrir avec succès ni $\mathtt{0}$ ni $\mathtt{1}$. Dans ces cas pathologiques, $\widetilde{C}'$ produit une mise en gage honnête à $\mathtt{0}$ et une chaîne quelconque comme "mise en gage" à $\mathtt{1}$. Il est facile de voir que $\widetilde{C}'$ vérifie les propriétés

$$
\begin{aligned}
\{A_{\widetilde{C}'}\}\mathrm{Prob}[E_0 \text{ ou } E_1] &= 1,\\
\{A_{\widetilde{C}'}\}\mathrm{Prob}[E_0 \text{ et } E_1] &\geq \{A_{\widetilde{C}}\}\mathrm{Prob}[E_0 \text{ et } E_1]
\end{aligned}
$$

où $A_{\widetilde{C}'}$ est défini d'une façon semblable à $A_{\widetilde{C}}$ en (2.12[38]). Évaluons la qualité de $\widetilde{C}'$ au sens de (2.13[38]):

$$
\begin{aligned}
\delta'(k) &= \{A_{\widetilde{C}'}\}(\mathrm{Prob}[E_0] + \mathrm{Prob}[E_1] - 1)\\
&= \{A_{\widetilde{C}'}\}(\mathrm{Prob}[E_0 \text{ ou } E_1] + \mathrm{Prob}[E_0 \text{ et } E_1] - 1)\\
&\geq 1 + \{A_{\widetilde{C}}\}\mathrm{Prob}[E_0 \text{ et } E_1] - 1\\
&= \delta(k).
\end{aligned}
$$

Autrement dit, étant donné un bon adversaire au sens de (2.11[37]), on peut construire un adversaire aussi bon, sinon meilleur, au sens de (2.13[38]) à un prix minime en temps d'exécution.

La conclusion est que les probabilités de succès (2.11[37]) et (2.13[38]) sont équivalentes à une réduction triviale près. Or, la ligne (2.13[38]) se relève beaucoup mieux au calcul quantique, et c'est d'elle dont nous nous inspirerons à la section 3.3[50] lorsque le temps sera venu de paramétrer la qualité d'un adversaire à condition liante d'une mise en gage quantique.

2.6 Lemmes utiles

Nous regroupons dans cette section divers lemmes techniques qui nous seront utiles aux chapitres 3 et suivants.

2.6.1 Propriété de $\mathsf{C}\text{-}\sigma_z{}^{\otimes k}$

La propriété élémentaire suivante de la transformation $\mathsf{C}\text{-}\sigma_z{}^{\otimes k}$ sera utilisée à la section 3.4[54]. Il s'agit simplement de calculer l'effet de $\mathsf{C}\text{-}\sigma_z{}^{\otimes k}$ sur une paire de chaînes de k bits.

Lemme 2.29 (*propriété de* $\mathsf{C}\text{-}\sigma_z{}^{\otimes k}$). Pour tout $\boldsymbol{w}_1$, $\boldsymbol{w}_2 \in \{\mathtt{0},\mathtt{1}\}^k$ on a

$$\mathsf{C}\text{-}\sigma_z{}^{\otimes k} \; |\boldsymbol{w}_1\rangle|\boldsymbol{w}_2\rangle = (-1)^{\boldsymbol{w}_1 \odot \boldsymbol{w}_2} \; |\boldsymbol{w}_1\rangle|\boldsymbol{w}_2\rangle$$

où l'exponentiation tensorielle ($^{\otimes k}$) est prise en parallèle, c'est-à-dire qu'un facteur $\mathsf{C}\text{-}\sigma_z$ est appliqué à deux bits de même position provenant de $\boldsymbol{w}_1$ et $\boldsymbol{w}_2$.

Preuve. Il suffit de remarquer que, pour deux bits b_1 et b_2,

$$\mathsf{C}\text{-}\sigma_z \; |b_1\rangle|b_2\rangle = (-1)^{b_1 \wedge b_2} \; |b_1\rangle|b_2\rangle,$$

et on obtient le calcul suivant:

$$\begin{aligned}
\mathsf{C}\text{-}\sigma_z{}^{\otimes k}\ |\boldsymbol{w}_1\rangle|\boldsymbol{w}_2\rangle &= \bigotimes_{j=1}^{k} \mathsf{C}\text{-}\sigma_z\ |\boldsymbol{w}_1[j]\rangle|\boldsymbol{w}_2[j]\rangle \\
&= \bigotimes_{j} (-1)^{\boldsymbol{w}_1[j]\wedge \boldsymbol{w}_2[j]}\ |\boldsymbol{w}_1[j]\rangle|\boldsymbol{w}_2[j]\rangle \\
&= \prod_{j} (-1)^{\boldsymbol{w}_1[j]\wedge \boldsymbol{w}_2[j]} \bigotimes_{j} |\boldsymbol{w}_1[j]\rangle|\boldsymbol{w}_2[j]\rangle \\
&= (-1)^{\boldsymbol{w}_1 \odot \boldsymbol{w}_2}\ |\boldsymbol{w}_1\rangle|\boldsymbol{w}_2\rangle.
\end{aligned}$$

■

2.6.2 Formule de changement de base

Le lemme qui suit nous donne une relation entre les éléments des bases canonique et diagonale, généralisant les lignes (2.1[26]) à (2.4[26]). Nous y faisons un usage abondant de la notation 2.11[27].

Lemme 2.30 (*formule de changement de base*). Soient $\boldsymbol{b} \in \{0,1\}^n$ et $\boldsymbol{\theta},\boldsymbol{w} \in \{+,\times\}^n$. On a

$$|\boldsymbol{b}\rangle_{\boldsymbol{\theta}} = \sum_{\boldsymbol{v}\,:\,\boldsymbol{v}\preceq \boldsymbol{w}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{w}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{v}}}{\sqrt{2}^{|\boldsymbol{w}|}} |\boldsymbol{b}\oplus\boldsymbol{v}\rangle_{\boldsymbol{\theta}\oplus\boldsymbol{w}}. \tag{2.14}$$

Preuve. Remarquons, par inspection, que la formule (2.14[41]) est valide si $n = 1$ et si $w = 1$, ce que nous pouvons écrire comme ceci, avec $b \in \{0,1\}$ et $\theta \in \{+,\times\}$:

$$|b\rangle_\theta = \sum_{v\in\{0,1\}} \frac{(-1)^{b\odot w\,\oplus\,b\odot v}}{\sqrt{2}} |b\oplus v\rangle_{\theta\oplus w}. \tag{2.15}$$

En ne considérant que les positions où $\boldsymbol{w}[j] = 1$ dans (2.14[41]) on peut écrire à l'aide de (2.15[41]):

$$\bigotimes_{j\in\mathrm{supp}(\boldsymbol{w})} |\boldsymbol{b}[j]\rangle_{\boldsymbol{\theta}[j]} = \bigotimes_{j\in\mathrm{supp}(\boldsymbol{w})} \left(\sum_{v\in\{0,1\}} \frac{(-1)^{\boldsymbol{b}[j]\odot\boldsymbol{w}[j]\,\oplus\,\boldsymbol{b}[j]\odot v}}{\sqrt{2}} |\boldsymbol{b}[j]\oplus v\rangle_{\boldsymbol{\theta}[j]\oplus\boldsymbol{w}[j]} \right).$$

Cette dernière expression est un produit de $|\boldsymbol{w}|$ facteurs, chacun d'eux étant une somme de 2 termes. La distributivité nous donne une somme de $2^{|\boldsymbol{w}|}$ termes qui sont des produits de $|\boldsymbol{w}|$ facteurs:

$$\begin{aligned}
&\bigotimes_{j\in\mathrm{supp}(\boldsymbol{w})} |\boldsymbol{b}[j]\rangle_{\boldsymbol{\theta}[j]} \\
&= \sum_{\boldsymbol{v}\,:\,\boldsymbol{v}\preceq\boldsymbol{w}} \left(\bigotimes_{j\in\mathrm{supp}(\boldsymbol{w})} \frac{(-1)^{\boldsymbol{b}[j]\odot\boldsymbol{w}[j]\,\oplus\,\boldsymbol{b}[j]\odot\boldsymbol{v}[j]}}{\sqrt{2}} |\boldsymbol{b}[j]\oplus\boldsymbol{v}[j]\rangle_{\boldsymbol{\theta}[j]\oplus\boldsymbol{w}[j]} \right) \\
&= \sum_{\boldsymbol{v}\,:\,\boldsymbol{v}\preceq\boldsymbol{w}} \frac{1}{\sqrt{2}^{|\boldsymbol{w}|}} \left(\prod_{j\in\mathrm{supp}(\boldsymbol{w})} (-1)^{\boldsymbol{b}[j]\odot\boldsymbol{w}[j]\,\oplus\,\boldsymbol{b}[j]\odot\boldsymbol{v}[j]} \bigotimes_{j\in\mathrm{supp}(\boldsymbol{w})} |\boldsymbol{b}[j]\oplus\boldsymbol{v}[j]\rangle_{\boldsymbol{\theta}[j]\oplus\boldsymbol{w}[j]} \right) \\
&= \sum_{\boldsymbol{v}\,:\,\boldsymbol{v}\preceq\boldsymbol{w}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{w}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{v}}}{\sqrt{2}^{|\boldsymbol{w}|}} \left(\bigotimes_{j\in\mathrm{supp}(\boldsymbol{w})} |\boldsymbol{b}[j]\oplus\boldsymbol{v}[j]\rangle_{\boldsymbol{\theta}[j]\oplus\boldsymbol{w}[j]} \right). \qquad (2.16)
\end{aligned}$$

D'autre part, si j est une position où $\boldsymbol{w}[j]=0$, et avec $\boldsymbol{v}\preceq\boldsymbol{w}$ on a $\boldsymbol{v}[j]=0$ aussi, on peut écrire trivialement:

$$\bigotimes_{j\notin\mathrm{supp}(\boldsymbol{w})} |\boldsymbol{b}[j]\rangle_{\boldsymbol{\theta}[j]} = \bigotimes_{j\notin\mathrm{supp}(\boldsymbol{w})} |\boldsymbol{b}[j]\oplus\boldsymbol{v}[j]\rangle_{\boldsymbol{\theta}[j]\oplus\boldsymbol{w}[j]}. \qquad (2.17)$$

De (2.16[42]) et (2.17[42]) on obtient facilement

$$|\boldsymbol{b}\rangle_{\boldsymbol{\theta}} = \sum_{\boldsymbol{v}\,:\,\boldsymbol{v}\preceq\boldsymbol{w}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{w}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{v}}}{\sqrt{2}^{|\boldsymbol{w}|}} |\boldsymbol{b}\oplus\boldsymbol{v}\rangle_{\boldsymbol{\theta}\oplus\boldsymbol{w}}$$

ce qui termine la preuve. ■

2.6.3 Transformation locale et décomposition de Schmidt

Le lemme suivant joue un rôle crucial dans la preuve de sécurité de la réduction 3.11[58]. Il permet d'affirmer que si deux états bipartites dans $\mathcal{H}^{\mathrm{A,B}}$ partagent les mêmes vecteurs de Schmidt du côté $\mathcal{H}^{\mathrm{B}}$ et si ces deux états peuvent être transformés l'un dans l'autre localement du côté $\mathcal{H}^{\mathrm{A}}$ par U, alors U transforme, les uns dans les autres, les vecteurs de Schmidt correspondants du côté $\mathcal{H}^{\mathrm{A}}$.

Lemme 2.31 (*transformation locale et décomposition de Schmidt*). Si

$$|\gamma\rangle^{\mathrm{A,B}} = \sum_j \vec{\mu}_j{}^{\mathrm{A}}\, |\beta_j\rangle^{\mathrm{B}}, \tag{2.18}$$

$$|\gamma'\rangle^{\mathrm{A,B}} = \sum_j \vec{\mu}'_j{}^{\mathrm{A}}\, |\beta_j\rangle^{\mathrm{B}}, \tag{2.19}$$

$$U^{\mathrm{A}} \otimes \mathbb{1}^{\mathrm{B}} \;:\; |\gamma\rangle \longmapsto |\gamma'\rangle, \tag{2.20}$$

où les états $\{|\beta_j\rangle\}$ sont linéairement indépendants, alors pour tout j on a

$$U \;:\; \vec{\mu}_j \longmapsto \vec{\mu}'_j.$$

Preuve. Il suffit de combiner les lignes (2.18[43]), (2.19[43]) et (2.20[43]) de la façon suivante:

$$\begin{aligned} 0 &= (U \otimes \mathbb{1})|\gamma\rangle - |\gamma'\rangle \\ &= \sum_j (U\vec{\mu}_j - \vec{\mu}'_j) \otimes |\beta_j\rangle \end{aligned}$$

et d'utiliser la proposition 2.17[30] pour obtenir la conclusion du lemme. ■

2.6.4 L'identité du parallélogramme et ses généralisations

Si $\vec{v}_0$ et $\vec{v}_1$ sont deux vecteurs quelconques d'un espace de Hilbert, alors on a l'identité facilement vérifiable suivante:

$$\frac{1}{2}(\|\vec{v}_0 + \vec{v}_1\|^2 + \|\vec{v}_0 - \vec{v}_1\|^2) = \|\vec{v}_0\|^2 + \|\vec{v}_1\|^2.$$

Cette identité est bien connue en géométrie euclidienne et s'appelle la *loi du parallélogramme*: *dans un parallélogramme, la somme des carrés des côtés est égale à la somme des carrés des diagonales.*

Cette identité possède une généralisation élégante aux dimensions supérieures. Soit $\{\vec{v}_{\boldsymbol{z}}\}_{\boldsymbol{z}\in\{0,1\}^n}$ une famille de vecteurs quelconques, alors:

$$\frac{1}{2^n}\sum_{\boldsymbol{w}\in\{0,1\}^n}\|\sum_{\boldsymbol{z}\in\{0,1\}^n}(-1)^{\boldsymbol{w}\odot\boldsymbol{z}}\vec{v}_{\boldsymbol{z}}\|^2=\sum_{\boldsymbol{z}}\|\vec{v}_{\boldsymbol{z}}\|^2. \tag{2.21}$$

On peut facilement démontrer cette identité par induction sur n, mais l'identité dont nous aurons besoin au chapitre 5 doit être un peu plus générale:

Lemme 2.32 (*identité du parallélogramme généralisée*). Soit $\{\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\}$ une famille de vecteurs doublement indexée par $\boldsymbol{w}\in\{0,1\}^n$ et $\boldsymbol{z}\in\{0,1\}^n$ qui satisfont la condition suivante:

$$\forall \boldsymbol{s},\boldsymbol{t}\in\{0,1\}^n,\text{ avec } \boldsymbol{s}\neq\boldsymbol{t}\ :$$

$$\sum_{\boldsymbol{w}}\ \sum_{z_1:\boldsymbol{w}\oplus z_1=\boldsymbol{s}}\ \sum_{z_2:\boldsymbol{w}\oplus z_2=\boldsymbol{t}}(-1)^{\boldsymbol{w}\odot(z_1\oplus z_2)}\langle\vec{v}_{\boldsymbol{w},z_1},\vec{v}_{\boldsymbol{w},z_2}\rangle=0, \tag{2.22}$$

alors

$$\sum_{\boldsymbol{w}}\|\sum_{\boldsymbol{z}}(-1)^{\boldsymbol{w}\odot\boldsymbol{z}}\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2=\sum_{\boldsymbol{w},\boldsymbol{z}}\|\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2.$$

Preuve. Calculons:

$$\begin{aligned}
&\sum_{\boldsymbol{w}}\|\sum_{\boldsymbol{z}}(-1)^{\boldsymbol{w}\odot\boldsymbol{z}}\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2\\
&= \sum_{\boldsymbol{w}}\langle\sum_{z_1}(-1)^{\boldsymbol{w}\odot z_1}\vec{v}_{\boldsymbol{w},z_1},\sum_{z_2}(-1)^{\boldsymbol{w}\odot z_2}\vec{v}_{\boldsymbol{w},z_2}\rangle\\
&= \sum_{\boldsymbol{w},z_1,z_2}(-1)^{\boldsymbol{w}\odot(z_1\oplus z_2)}\langle\vec{v}_{\boldsymbol{w},z_1},\vec{v}_{\boldsymbol{w},z_2}\rangle\\
&= \sum_{\boldsymbol{w},\boldsymbol{z}}\|\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2+\sum_{\boldsymbol{w},z_1,z_2:z_1\neq z_2}(-1)^{\boldsymbol{w}\odot(z_1\oplus z_2)}\langle\vec{v}_{\boldsymbol{w},z_1},\vec{v}_{\boldsymbol{w},z_2}\rangle. \qquad (2.23)
\end{aligned}$$

On change l'ordre des termes de la somme à droite en introduisant les variables de sommation $\boldsymbol{s}$ et $\boldsymbol{t}$:

$$\sum_{\boldsymbol{w},z_1,z_2:z_1\neq z_2}(-1)^{\boldsymbol{w}\odot(z_1\oplus z_2)}\langle\vec{v}_{\boldsymbol{w},z_1},\vec{v}_{\boldsymbol{w},z_2}\rangle$$

$$
\begin{aligned}
&= \sum_{\boldsymbol{w}} \sum_{\boldsymbol{z}_1} \sum_{\boldsymbol{s}:\boldsymbol{w}\oplus \boldsymbol{z}_1=\boldsymbol{s}} \sum_{\boldsymbol{z}_2:\boldsymbol{z}_1\neq \boldsymbol{z}_2} \sum_{\boldsymbol{t}:\boldsymbol{w}\oplus \boldsymbol{z}_2=\boldsymbol{t}} (-1)^{\boldsymbol{w}\odot(\boldsymbol{z}_1\oplus \boldsymbol{z}_2)} \langle \vec{v}_{\boldsymbol{w},\boldsymbol{z}_1}, \vec{v}_{\boldsymbol{w},\boldsymbol{z}_2}\rangle \\
&= \sum_{\boldsymbol{s},\boldsymbol{t}:\boldsymbol{s}\neq \boldsymbol{t}} \sum_{\boldsymbol{w}} \sum_{\boldsymbol{z}_1:\boldsymbol{w}\oplus \boldsymbol{z}_1=\boldsymbol{s}} \sum_{\boldsymbol{z}_2:\boldsymbol{w}\oplus \boldsymbol{z}_2=\boldsymbol{t}} (-1)^{\boldsymbol{w}\odot(\boldsymbol{z}_1\oplus \boldsymbol{z}_2)} \langle \vec{v}_{\boldsymbol{w},\boldsymbol{z}_1}, \vec{v}_{\boldsymbol{w},\boldsymbol{z}_2}\rangle \\
&= \sum_{\boldsymbol{s},\boldsymbol{t}:\boldsymbol{s}\neq \boldsymbol{t}} 0 \qquad (2.24) \\
&= 0
\end{aligned}
$$

où l'équation (2.24[45]) est obtenue de la condition (2.22[44]) du théorème. Il suffit maintenant de remplacer ce dernier 0 dans l'équation (2.23[44]) pour obtenir le résultat annoncé. ■

On pourra vérifier que le lemme 2.32[44] est bien une généralisation de l'identité (2.21[44]) pour la famille $\{\vec{u}_{\boldsymbol{y}}\}_{\boldsymbol{y}\in\{0,1\}^n}$ en posant $\vec{v}_{\boldsymbol{w},\boldsymbol{z}} \equiv \vec{u}_{\boldsymbol{w}\oplus \boldsymbol{z}}$.

Enfin, généralisons une dernière fois:

Lemme 2.33 (*corollaire du lemme 2.32*[44]). Soit $A \subseteq \{0,1\}^n$ un ensemble de chaînes de bits. Soit $\{\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\}$ une famille de vecteurs doublement indexée par $\boldsymbol{w} \in \{0,1\}^n$ et $\boldsymbol{z} \in A$ qui satisfont:

$$
\begin{aligned}
&\forall \boldsymbol{s},\boldsymbol{t} \in \{0,1\}^n, \text{ avec } \boldsymbol{s} \neq \boldsymbol{t} \;: \\
&\sum_{\boldsymbol{w}} \sum_{\boldsymbol{z}_1\in A:\boldsymbol{w}\oplus \boldsymbol{z}_1=\boldsymbol{s}} \sum_{\boldsymbol{z}_2\in A:\boldsymbol{w}\oplus \boldsymbol{z}_2=\boldsymbol{t}} (-1)^{\boldsymbol{w}\odot(\boldsymbol{z}_1\oplus \boldsymbol{z}_2)} \langle \vec{v}_{\boldsymbol{w},\boldsymbol{z}_1}, \vec{v}_{\boldsymbol{w},\boldsymbol{z}_2}\rangle = 0, \qquad (2.25)
\end{aligned}
$$

alors

$$\sum_{\boldsymbol{w}} \|\sum_{\boldsymbol{z}\in A} (-1)^{\boldsymbol{w}\odot \boldsymbol{z}} \vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2 = \sum_{\boldsymbol{w}\in\{0,1\}^n, \boldsymbol{z}\in A} \|\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2.$$

Preuve. Posons $\vec{v}_{\boldsymbol{w},\boldsymbol{z}} \equiv 0$ pour $\boldsymbol{z} \notin A$ afin de former une famille complète. On peut vérifier que la condition du lemme 2.32[44] est satisfaite et que de sa conclusion découle celle de ce corollaire. ■

Chapitre 3

Mise en gage à partir d'une permutation à sens unique quantique

La première composante de notre travail consiste à montrer qu'une mise en gage est possible si l'on souscrit à une certaine hypothèse calculatoire quantique. Plus précisément, nous contruisons une mise en gage camouflante à partir d'une famille de permutations à sens unique — rappelons que ce résultat est le sujet de l'article [DMS00]. La mise en gage sera de surcroît non interactive (un seul message est transmis d'Alice à Bob lors des phases d'engagement ou d'ouverture) et parfaitement camouflante. Nous devons donc définir les termes de l'exposé: les notions de permutation à sens unique et de mise en gage comme primitives cryptographiques. Nous nous attarderons uniquement à modéliser les mises en gage *non interactives* et *parfaitement camouflantes*, non pas qu'un modèle plus général serait inintéressant, mais plutôt parce que ce modèle restreint suffit aux besoins de notre exposé.

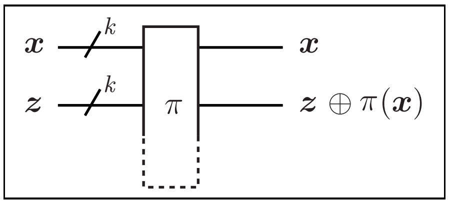


FIG. 3.1 – *Permutation: modélisation quantique*

3.1 Permutation à sens unique quantique (QOWP)

Une permutation à sens unique, c'est avant tout une famille de permutations sur les ensembles $\{0,1\}^k$. Pour $k > 0$ fixé, le circuit est illustré à la figure 3.1[47].

Remarquons qu'il aurait été futile de modéliser notre fonction par une porte qui prend en entrée uniquement la chaîne $\boldsymbol{x}$ de taille k et qui donne en sortie $\pi(\boldsymbol{x})$, car il s'agirait toujours d'une permutation facile à inverser. En effet, un tel objet possède trivialement un inverseur efficace: il suffit d'inverser l'ordre d'exécution des composantes tout en inversant chaque composante. Le circuit résultant contient le même nombre de portes élémentaires que le circuit original. Il est donc nécessaire que la porte π prenne $2k$ bits en entrée, et accessoirement un registre de travail, et que $\boldsymbol{x}$ soit recopié en sortie. Pour compléter la définition de la transformation unitaire π, si le registre ancillaire contient autre chose que 0^k, disons $\boldsymbol{z} \in \{0,1\}^k$, alors la sortie correspondante sera $\boldsymbol{z} \oplus \pi(\boldsymbol{x})$ au lieu de $\pi(\boldsymbol{x})$. Cette discussion nous amène à la définition qui suit.

Définition 3.1 (*permutation à sens unique*). Une famille de permutations

$$\pi = \{\pi_k\}_{k>0}$$

$$\pi_k : \{0,1\}^k \longrightarrow \{0,1\}^k$$

calculable en temps poly(k) par une famille de circuits quantiques répondant aux spécifications de la figure 3.1[47] (où la lettre π désigne à la fois la permutation et

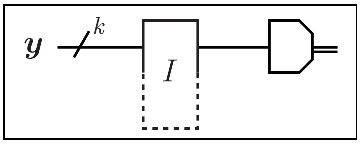


FIG. 3.2 – *Permutation à sens unique: adversaire*

le circuit qui l'implante) est dite *à sens unique* lorsqu'elle est considérée avec la notion d'adversaire suivante:

$$I = \{I_k\}_{k>0}$$

est un adversaire $(t(k),s(k))$-bon si

- I est une famille de circuits quantiques de taille $O(t(k))$ satisfaisant les spécifications de la figure 3.2[48];
- $\{\ \boldsymbol{x} \xleftarrow{\mathcal{U}} \{0,1\}^k;\ \boldsymbol{x}' \xleftarrow{\mathbb{M}_+^{\otimes k}} I|\pi(\boldsymbol{x})\rangle\ \}\mathrm{Prob}[\boldsymbol{x}' = \boldsymbol{x}]\ \geq\ s(k)$.

La probabilité ci-dessus est appelée la *probabilité de succès* de I. L'entier k sert de paramètre de sécurité. Si la probabilité de succès de l'inverseur est 1, alors on dira que l'inverseur est *parfait*. ▲

Un adversaire à la permutation π est donc un inverseur I. La sortie de l'inverseur sera $\pi^{-1}(\boldsymbol{y})$, c'est-à-dire que l'on observera $\pi^{-1}(\boldsymbol{y})$ avec une certaine probabilité à la sortie du registre supérieur de la figure 3.2[48] lorsque mesuré dans la base canonique et lorsque $\boldsymbol{y}$ est choisi uniformément au hasard.

Le sens le plus courant donné à l'expression *permutation à sens unique* correspond à une famille de permutations π qui ne possède pas d'adversaire $(t(k),s(k))$-bon pour $t(k) \in \mathrm{poly}(k)$ et pour $s(k) \notin \mathrm{negl}(k)$, c'est-à-dire π ne possède pas d'adversaire *efficace* ayant probabilité de succès *non négligeable*. Dans [Gol98] on propose une notion de fonction à sens unique *faible* (*weak one-way function*) qui revient à dire que π ne possède pas d'adversaire $(t(k),s(k))$-bon pour $t(k) \in \mathrm{poly}(k)$ et pour

$1 - s(k) \in \mathrm{negl}(k)$. L'avantage de paramétrer la qualité des adversaires au moyen de la paire $(t(k),s(k))$ vient du gain en généralité et de la possibilité de quantifier les pertes encourues, en efficacité et en probabilité de succès, lors d'une réduction d'un adversaire à un autre. Cette approche est inspirée par celle de Luby [Lub96] qui s'en remet parfois à la quantité $t(k)/s(k)$ qu'il appelle le *time-success ratio* de l'adversaire.

La définition 3.1[47] est certainement la plus simple, mais elle n'est pas la plus générale ou la seule définition que nous aurions pu adopter. En effet, lorsque le temps est venu d'implanter une permutation dans un cas particulier, il n'est pas rare que l'on ne puisse pas donner un sens à l'expression $\pi_k(\boldsymbol{x})$ pour tous les $\boldsymbol{x} \in \{0,1\}^k$, pour tous les $k > 0$, ou même pour tous les k au-delà d'un certain seuil k_0. Ces difficultés peuvent généralement être surmontées au moyen d'artifices techniques, du moment que la permutation est bien définie pour une infinité de valeurs de k, voir [Gol98].

3.2 La question des candidats

Nous nous apprêtons à fonder une mise en gage, et plus tard un transfert inconscient, sur la primitive QOWP. Une question naturelle vient à l'esprit: y a-t-il des permutations à sens unique quantique, et si oui, quelles sont-elles? Jusqu'à un certain point, l'état des choses en cryptographie quantique ressemble à l'état de notre ignorance en cryptographie classique: nul ne sait si les permutations à sens unique existent.

Là où les situations quantiques et classiques diffèrent, c'est sur l'existence de bons candidats. Le calcul classique jouit d'une longue tradition qui remonte à l'algorithme d'Euclide. Si encore à ce jour aucun algorithme efficace n'a été découvert pour le problème de la factorisation, il est raisonnable de supposer qu'il s'agit effectivement d'un problème difficile et qu'un bon candidat au titre de fonction à sens unique peut être construit sur le problème de la factorisation. En quantique, la problématique est double. D'une part l'algorithmique quantique ne jouit pas d'une aussi longue tradition, et d'autre part pendant ses quelques années d'existence on a réussi à résoudre les problèmes de la factorisation et du logarithme discret, les deux problèmes supposés difficiles sur lesquels reposent la plupart des systèmes cryptographiques classiques en usage actuellement [Sho97]. On consultera [Zhu01] pour une vue d'ensemble des problèmes difficiles pouvant être utilisés ou non en cryptographie quantique et s'ils donnent lieu à une fonction ou à une permutation à sens unique, avec brèche ou non. Les domaines prometteurs suivants sont identifiés par Zhu afin de formuler des hypothèses calculatoires viables dans le monde quantique:

- la théorie des codes;
- le problème de la sous-somme (*subset sum, knapsack*);
- le problème du sous-produit (*subset product*);
- la théorie des treillis (*lattices*);
- la théorie combinatoire des groupes.

3.3 Mise en gage quantique inconditionnellement camouflante ($\mathsf{BC_H}$)

La modélisation d'une mise en gage au moyen d'un circuit quantique apparaît à la figure 3.3[51]. Ce modèle est *non interactif* parce qu'un seul message est transmis, d'Alice vers Bob, lors de l'engagement. Le circuit C est le circuit d'engagement qui produit un certain état qui dépend du bit b qu'Alice désire engager. Le contenu quantique du registre $\mathcal{H}^{\text{Bob}}$ est transmis lors de l'engagement, les regitres $\mathcal{H}^{\text{b,Alice}}$

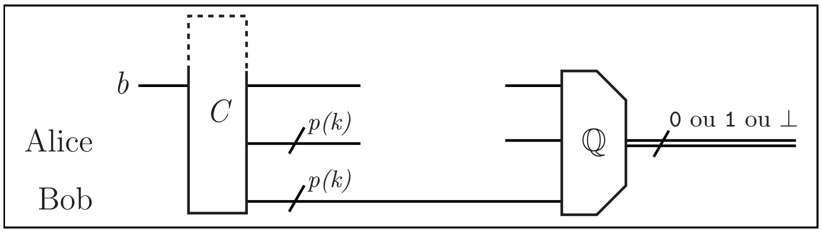


FIG. 3.3 – *Mise en gage non interactive: modélisation quantique*

ne seront envoyés qu'à l'ouverture, ce qui est indiqué dans le diagramme par des fils quantiques oblitérés. Ces deux portions restent a priori intriquées entre l'engagement et l'ouverture. La porte $\mathbb{Q}$ est une mesure exécutée par Bob à l'ouverture. Trois résultats sont possibles: $\mathtt{0}$ ou $\mathtt{1}$ signifient que Bob accepte qu'Alice s'était honnêtement engagée à la valeur lue, et $\perp$ est un message d'erreur indiquant à Bob que le protocole échoue pour cause de malhonnêteté de la part d'Alice, ce qui inclut la possibilité d'un refus d'ouvrir. Nous n'indiquons aucun travail accompli par Alice entre l'engagement et l'ouverture car ces calculs peuvent être incorporés à la porte C sans perte de généralité. La taille des registres $\mathcal{H}^{\text{Alice}}$ et $\mathcal{H}^{\text{Bob}}$ est polynômiale en un paramètre de sécurité k. Le scénario que nous venons de décrire s'exprime formellement par la définition qui suit.

Définition 3.2 (*mise en gage non interactive quantique: complétude*). Un schème de *mise en gage non interactive quantique* est donné par une paire de familles de circuits quantiques de tailles polynômiales

$$C = \{C_k\}_{k>0},\ \ \mathbb{Q} = \{\mathbb{Q}_k\}_{k>0}$$

$$\mathbb{Q}_k = [\mathbb{Q}_{k,0},\, \mathbb{Q}_{k,1},\, \mathbb{Q}_{k,\perp}]$$

répondant aux spécifications de la figure 3.3[51]. De plus, le circuit doit satisfaire la condition

$$\forall b \in \{\mathtt{0},\mathtt{1}\}\ :\ \{\ b' \overset{\mathbb{Q}}{\leftarrow} C|b\rangle\ \}\mathrm{Prob}[b' = b]\ =\ 1 \qquad (3.1)$$

ce que nous appelons une condition de *complétude*. ▲

Remarque 3.3 (*probabilité de succès*). On a l'identité

$$\{\ b' \overset{\mathbb{Q}}{\leftarrow} |\psi\rangle\ \}\mathrm{Prob}[b' = b''] \quad = \quad \|\mathbb{Q}_{b''}|\psi\rangle\|^2$$

pour tout $b'' \in \{0,1\}$ et pour tout état $|\psi\rangle$, et cette quantité est la probabilité d'ouvrir le bit b'' avec succès étant donnée la préparation $|\psi\rangle$, voir la ligne (2.6[28]) et la proposition 2.18[31]. ▲

La condition de complétude sur C et $\mathbb{Q}$ revient à stipuler qu'une mise en gage honnête sera ouverte avec succès. Une définition un peu plus générale, dont nous ne nous embarrasserons pas, serait de permettre une probabilité d'échec négligeable en k à l'équation (3.1[51]).

Puisque la mise en gage que nous allons construire sera parfaitement camouflante, nous n'aurons besoin de définir que l'adversaire à la condition liante. Nous donnons une définition positive du côté parfaitement camouflant, c'est-à-dire en ne faisant pas appel à la notion d'adversaire:

Définition 3.4 (*mise en gage quantique: camouflage parfait*). Une mise en gage quantique telle que modélisée à la définition 3.2[51] est *parfaitement camouflante* si, immédiatement après l'éxécution de la porte C, la matrice de densité de l'état restreint au registre $\mathcal{H}^{\mathrm{Bob}}$ est la même quelle que soit la valeur de $b \in \{0,1\}$. Formellement:

$$\mathrm{tr}_{\mathrm{Alice,Etc}}(C|0\rangle\langle 0|C^\dagger) = \mathrm{tr}_{\mathrm{Alice,Etc}}(C|1\rangle\langle 1|C^\dagger) \tag{3.2}$$

où l'espace $\mathcal{H}^{\mathrm{Etc}}$ correspond à tous les registres situés au-dessus de $\mathcal{H}^{\mathrm{Alice}}$ dans la figure 3.3[51]. ▲

En s'inspirant de la modélisation classique de la section 2.5.2[38] et de la discussion qui s'y trouve, l'adversaire à la condition liante de la mise en gage est illustré à la figure 3.4[53]. Le circuit $\widetilde{C}$ implante un faux engagement, ou un engagement

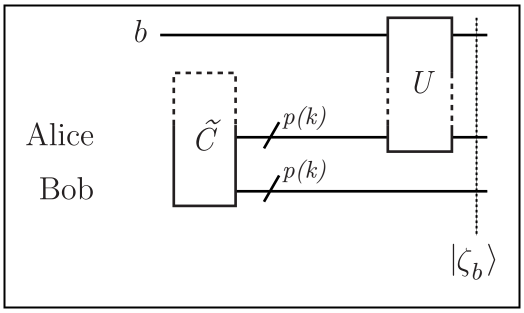


FIG. 3.4 – *Mise en gage quantique non interactive: adversaire à la condition liante*

malhonnête, et l'état qui est produit à la sortie de cette porte ne dépend pas de la valeur d'aucun bit b. Il peut cependant être transformé en un état $|\zeta_0\rangle$ ou $|\zeta_1\rangle$, selon la volonté du tricheur, à l'aide de la transformation U qui n'agit que sur les registres disponibles du côté d'Alice une fois la mise en gage transmise à Bob. La qualité d'un tel attaquant est formalisée par la définition 3.5[53].

Définition 3.5 (*mise en gage quantique: adversaire à la condition liante*). Un *adversaire à la condition liante* d'une mise en gage quantique telle que modélisée à la définition 3.2[51] est une paire de familles de circuits quantiques

$$\widetilde{C} = \{\widetilde{C}_k\}_{k>0},\ U = \{U_k\}_{k>0}$$

qui répondent aux spécifications de la figure 3.4[53]. Un tel adversaire est $(t(k),s(k))$-bon si

$$\|\widetilde{C}\|_{\mathcal{U}} + \|U\|_{\mathcal{U}} \in O(t(k)),$$

$$\|\mathbb{Q}_0\,|\zeta_0\rangle\|^2 + \|\mathbb{Q}_1\,|\zeta_1\rangle\|^2 - 1 \geq s(k).$$

L'entier k sert de paramètre de sécurité. Si $\|\mathbb{Q}_0\,|\zeta_0\rangle\|^2 + \|\mathbb{Q}_1\,|\zeta_1\rangle\|^2 = 2$, alors on dira que l'adversaire est *parfait.* ▲

La remarque suivante donne une borne inférieure sur la qualité d'un adversaire pour qu'il soit considéré non trivial.

Remarque 3.6 (*adversaire trivial*). La paire $(\widetilde{C},U) \equiv (C_{b\leftarrow 0},\mathbb{1})$ est un adversaire

$(\|C\|_{\mathcal{U}}, 0)$-bon, où $C_{b\leftarrow 0}$ est la transformation obtenue de C en fixant l'input b à $\mathsf{0}$ dans la figure 3.3[51]. ▲

Autrement dit, on peut réaliser une "attaque" $(\|C\|_{\mathcal{U}},0)$-bonne en n'utilisant aucune ressource qui ne soit accessible à un participant honnête.

La terminologie suivante sera abondamment utilisée et nous en faisons une définition distincte.

Définition 3.7 (*incarner une attaque*). Deux familles d'états $\{|\zeta_{0,k}\rangle\}_{k>0}$ et $\{|\zeta_{1,k}\rangle\}_{k>0}$, ou par abus de langage deux états $|\zeta_{\mathsf{0}}\rangle$ et $|\zeta_{\mathsf{1}}\rangle$, *incarnent* une attaque contre la condition liante d'une mise en gage telle que modélisée à la définition 3.2[51], s'ils sont issus d'une paire de circuits $(\widetilde{C},U)$ comme à la figure 3.4[53]. ▲

3.4 La réduction

Tous les ingrédients ont été préparés, nous sommes prêts à présenter la réduction.

Réduction 3.8 ($\mathsf{BC_H} \leq \mathsf{QOWP}$). Soit π une permutation à sens unique telle que décrite à la définition 3.1[47]. La réduction apparaît à la figure 3.5[55], où $\mathbb{P} = [\mathbb{P}_{\mathsf{0}},\mathbb{P}_{\mathsf{1}},\mathbb{P}_{\perp}]$ est définie par

$$\begin{aligned}
\mathbb{P}_{\mathsf{0}} &= \sum_{\boldsymbol{x}\in\{\mathsf{0},\mathsf{1}\}^k} |\mathsf{0}\rangle\langle\mathsf{0}| \otimes |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes |\pi(\boldsymbol{x})\rangle\langle\pi(\boldsymbol{x})|,\\
\mathbb{P}_{\mathsf{1}} &= \sum_{\boldsymbol{x}\in\{\mathsf{0},\mathsf{1}\}^k} |\mathsf{1}\rangle\langle\mathsf{1}| \otimes |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes |\pi(\boldsymbol{x})\rangle_{\times}\langle\pi(\boldsymbol{x})|,\\
\mathbb{P}_{\perp} &= \mathbb{1} - \mathbb{P}_{\mathsf{0}} - \mathbb{P}_{\mathsf{1}}.
\end{aligned}$$

La mesure $\mathbb{P}$ est bien définie, c'est-à-dire qu'elle est bien constituée de trois projecteurs orthogonaux deux à deux dont la somme est l'identité. ▲

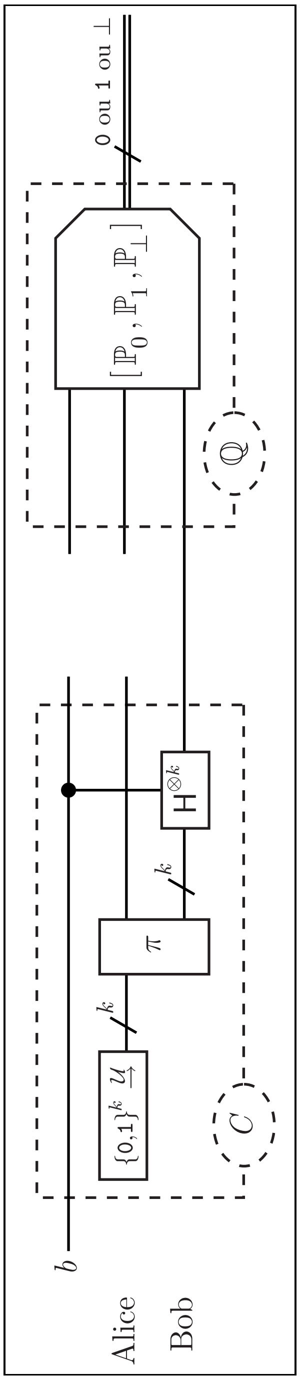


FIG. 3.5 – $\mathsf{BC_H} \leq \mathsf{QOWP}$

L'engagement au bit b consiste à choisir uniformément au hasard une chaîne $\boldsymbol{x} \in \{\mathtt{0},\mathtt{1}\}^k$ et de calculer son image $\pi(\boldsymbol{x})$. Celle-ci est ensuite transmise à Bob dans la base canonique si $b = \mathtt{0}$ ou dans la base diagonale si $b = \mathtt{1}$. À l'ouverture, Alice transmet b et $\boldsymbol{x}$, et Bob vérifie qu'il avait bien reçu $\pi(\boldsymbol{x})$ dans la base indiquée par b. Il est facile de vérifier que schème est complet et parfaitement camouflant, ce qui est l'objet de nos deux premiers théorèmes.

Théorème 3.9 (*complétude du schème de la réduction 3.8*[54]). Le schème de mise en gage décrit à la réduction 3.8[54] est complet, au sens de la définition 3.2[51].

Preuve. On peut facilement vérifier que les circuits C et $\mathbb{Q}$ de la figure 3.5[55] sont de taille polynômiale en k, puisque qu'ils ne font appel qu'au circuit π, qui par hypothèse est de taille polynômiale, à un nombre linéaire de porte H ou $\mathsf{C\text{-}H}$, et au choix aléatoire $\boldsymbol{x} \stackrel{\mathcal{U}}{\leftarrow} \{\mathtt{0},\mathtt{1}\}^k$ qui peut être implanté avec un nombre linéaire de porte H. Vérifions la condition (3.1[51]), soit $b \in \{\mathtt{0},\mathtt{1}\}$:

$$
\begin{aligned}
&\{\ b' \stackrel{\mathbb{Q}}{\leftarrow} C|b\rangle\ \}\mathrm{Prob}[b' = b] \\
&\quad = \quad \{ \quad \boldsymbol{x} \stackrel{\mathcal{U}}{\leftarrow} \{\mathtt{0},\mathtt{1}\}^k; \\
&\qquad\qquad\quad b' \stackrel{\mathbb{P}}{\leftarrow} |b\rangle|\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle_b \quad \}\mathrm{Prob}[b' = b] \\
&\quad = \sum_{\boldsymbol{x}\in\{\mathtt{0},\mathtt{1}\}^k} \frac{1}{2^k} \|\mathbb{P}_b\ |b\rangle|\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle_b\|^2 \qquad \text{(par la remarque 3.3[52])} \\
&\quad = \sum_{\boldsymbol{x}} \frac{1}{2^k} \left\| \left(\sum_{\boldsymbol{x}'\in\{\mathtt{0},\mathtt{1}\}^k} |b\rangle\langle b| \otimes |\boldsymbol{x}'\rangle\langle\boldsymbol{x}'| \otimes |\pi(\boldsymbol{x}')\rangle_b\langle\pi(\boldsymbol{x}')| \right) |b\rangle|\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle_b \right\|^2 \\
&\quad = \sum_{\boldsymbol{x}} \frac{1}{2^k} \||b\rangle|\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle_b\|^2 \\
&\quad = \sum_{\boldsymbol{x}} \frac{1}{2^k} \\
&\quad = 1
\end{aligned}
$$

■

Théorème 3.10 (*camouflage parfait du schème de la réduction 3.8*[54]). Le schème de mise en gage décrit à la réduction 3.8[54] est parfaitement camouflant.

Preuve. Nous devons calculer les deux membres de l'équation (3.2[52]) et vérifier qu'ils sont égaux. En fait, en examinant la figure 3.5[55], on se rend compte que Bob reçoit un état parfaitement mélangé à la sortie de C, puisqu'il ignore encore la valeur de $\boldsymbol{x}$. Formellement, on a d'une part:

$$\begin{aligned}
\mathrm{tr}_{\mathrm{Alice,Etc}}(C|\mathtt{0}\rangle\langle\mathtt{0}|C^\dagger) &= \sum_{\boldsymbol{x}\in\{\mathtt{0},\mathtt{1}\}^k} \frac{1}{2^k}|\pi(\boldsymbol{x})\rangle\langle\pi(\boldsymbol{x})| \\
&\boxed{\begin{array}{l} \boldsymbol{y} \equiv \pi(\boldsymbol{x}) \\ \boldsymbol{x} = \pi^{-1}(\boldsymbol{y}) \end{array}} \\
&= \sum_{\boldsymbol{y}\in\{\mathtt{0},\mathtt{1}\}^k} \frac{1}{2^k}|\boldsymbol{y}\rangle\langle\boldsymbol{y}| \\
&= \frac{1}{2^k}\mathbb{1}_{2^k},
\end{aligned}$$

et d'autre part:

$$\begin{aligned}
\mathrm{tr}_{\mathrm{Alice,Etc}}(C|\mathtt{1}\rangle\langle\mathtt{1}|C^\dagger) &= \sum_{\boldsymbol{x}\in\{\mathtt{0},\mathtt{1}\}^k} \frac{1}{2^k}|\pi(\boldsymbol{x})\rangle_\times\langle\pi(\boldsymbol{x})| \\
&\boxed{\begin{array}{l} \boldsymbol{y} \equiv \pi(\boldsymbol{x}) \\ \boldsymbol{x} = \pi^{-1}(\boldsymbol{y}) \end{array}} \\
&= \sum_{\boldsymbol{y}\in\{\mathtt{0},\mathtt{1}\}^k} \frac{1}{2^k}|\boldsymbol{y}\rangle_\times\langle\boldsymbol{y}| \\
&= \sum_{\boldsymbol{y}} \frac{1}{2^k}\mathsf{H}^{\otimes k}|\boldsymbol{y}\rangle\langle\boldsymbol{y}|\mathsf{H}^{\otimes k} \\
&= \frac{1}{2^k}\mathsf{H}^{\otimes k}\left(\sum_{\boldsymbol{y}}|\boldsymbol{y}\rangle\langle\boldsymbol{y}|\right)\mathsf{H}^{\otimes k} \\
&= \frac{1}{2^k}\mathbb{1}_{2^k}.
\end{aligned}$$

■

On remarque que la première utilisation du fait que π est une permutation sur $\{0,1\}^k$ survient dans la preuve de ce théorème.

Nous devons maintenant examiner le côté liant de la mise en gage décrite à la réduction 3.8[54]. Comme la sécurité de ce côté est calculatoire, nous réduisons un attaquant à QOWP à un attaquant à la condition liante de $\mathsf{BC_H}$. Dit autrement, nous construisons un inverseur de π à partir d'un circuit d'attaque à la condition liante de notre mise en gage. Pour des raisons techniques, nous séparons les cas *parfait* et *imparfait*, c'est-à-dire que nous considérons d'abord un attaquant à $\mathsf{BC_H}$ parfait au sens de la définition 3.5[53]. Cette séparation des cas a aussi une vertu pédagogique parce que le cas parfait est plus simple à traiter et qu'il permet de faire ressortir l'essence de la réduction.

Réduction 3.11 ($\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC_H}}$, *cas parfait*). Soient $\widetilde{C}$ et U deux familles de circuits tels que décrits à la définition 3.5[53], attaquant le $\mathsf{BC_H}$ de la réduction 3.8[54]. Nous supposons que cette attaque est parfaite, c'est-à-dire:

$$||\mathbb{P}_0|\zeta_0\rangle||^2 = ||\mathbb{P}_1|\zeta_1\rangle||^2 = 1$$

où $|\zeta_0\rangle$ et $|\zeta_1\rangle$ sont les états pouvant être produits par une Alice malhonnête dans le but d'ouvrir 0 ou 1, voir la définition 3.5[53]. Les projecteurs $\mathbb{P}_0$ et $\mathbb{P}_1$ sont définis à la réduction 3.8[54]. La construction d'un inverseur pour la permutation π apparaît à la figure 3.6[59], voir la section 2.3.3[25] pour une définition des portes C-σ_z et σ_x utilisées dans ce circuit. ▲

Simplifions d'abord le circuit de la figure 3.6[59] en introduisant les portes C_0 et $U_{0\to 1}$, ce qui est illustré à la figure 3.7[60]. La porte C_0 remplace $U\widetilde{C}$, pour produire l'état $|\zeta_0\rangle$, voir la figure 3.4[53]:

$$C_0|\vdash\rangle = |\zeta_0\rangle, \tag{3.3}$$

et $U_{0\to 1}$ remplace $U\sigma_x U^\dagger$, pour transformer $|\zeta_0\rangle$ en $|\zeta_1\rangle$, voir encore la figure 3.4[53]:

$$(U_{0\to 1} \otimes \mathbb{1}^{\mathrm{Bob}})|\zeta_0\rangle = |\zeta_1\rangle. \tag{3.4}$$

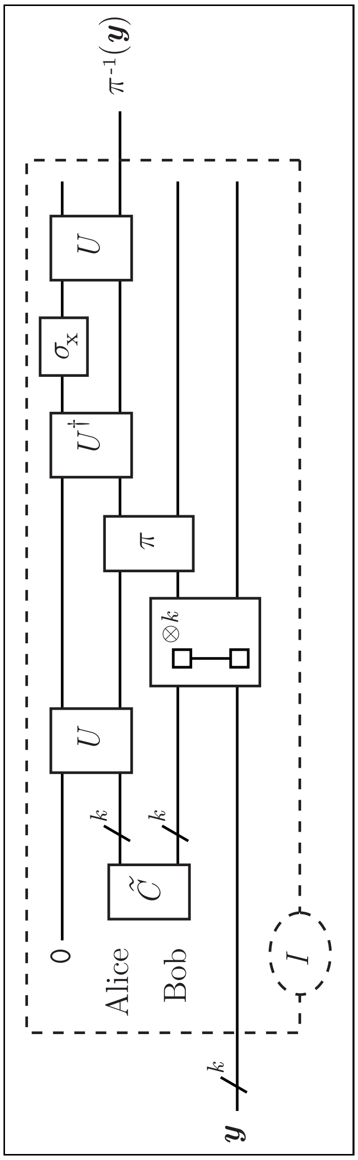


FIG. 3.6 – $\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC_H}}$, *cas parfait*

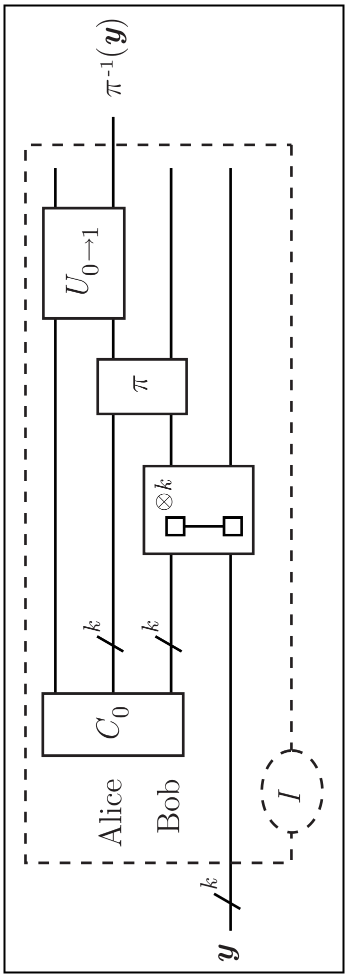


Fig. 3.7 – $\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC_H}}$, *cas parfait, circuit simplifié*

Avant de plonger dans la démonstration que le circuit de la figure 3.7[60] produit bien $\pi^{-1}(\boldsymbol{y})$, nous avons besoin de deux remarques et d'un lemme.

Remarque 3.12 (*propriété de* $|\zeta_0\rangle$). Puisque $\|\mathbb{P}_0|\zeta_0\rangle\|^2 = 1$, il suffit d'inspecter la définition du projecteur $\mathbb{P}_0$ à la réduction 3.8[54] pour conclure que $|\zeta_0\rangle$ doit nécessairement être de la forme

$$|\zeta_0\rangle \equiv \sum_{\boldsymbol{x}\in\{0,1\}^k} \vec{\lambda}_{0,\boldsymbol{x}}|\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle. \tag{3.5}$$

Par la formule de changement de base (lemme 2.30[41]) on peut écrire

$$= \sum_{\boldsymbol{x}} \sum_{\boldsymbol{v}\in\{0,1\}^k} \frac{(-1)^{\boldsymbol{v}\odot\pi(\boldsymbol{x})}}{\sqrt{2}^k}\vec{\lambda}_{0,\boldsymbol{x}}|\boldsymbol{x}\rangle|\boldsymbol{v}\rangle_\times$$

$$= \sum_{\boldsymbol{v}} \frac{1}{\sqrt{2}^k}\left(\sum_{\boldsymbol{x}}(-1)^{\boldsymbol{v}\odot\pi(\boldsymbol{x})}\vec{\lambda}_{0,\boldsymbol{x}}|\boldsymbol{x}\rangle\right)|\boldsymbol{v}\rangle_\times$$

$$\boxed{|\xi(\boldsymbol{v})\rangle \equiv \sum_{\boldsymbol{x}}(-1)^{\boldsymbol{v}\odot\pi(\boldsymbol{x})}\vec{\lambda}_{0,\boldsymbol{x}}|\boldsymbol{x}\rangle} \tag{3.6}$$

$$= \sum_{\boldsymbol{v}} \frac{1}{\sqrt{2}^k}|\xi(\boldsymbol{v})\rangle|\boldsymbol{v}\rangle_\times. \tag{3.7}$$

▲

Remarque 3.13 (*propriété de* $|\zeta_1\rangle$). Comme $\|\mathbb{P}_1|\zeta_1\rangle\|^2 = 1$, nous écrivons

$$|\zeta_1\rangle \equiv \sum_{\boldsymbol{x}\in\{0,1\}^k} \vec{\lambda}_{1,\boldsymbol{x}}|\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle_\times$$

$$\boxed{\begin{array}{l}\boldsymbol{v} \equiv \pi(\boldsymbol{x})\\ \boldsymbol{x} = \pi^{-1}(\boldsymbol{v})\end{array}}$$

$$= \sum_{\boldsymbol{v}\in\{0,1\}^k} \vec{\lambda}_{1,\pi^{-1}(\boldsymbol{v})}|\pi^{-1}(\boldsymbol{v})\rangle|\boldsymbol{v}\rangle_\times. \tag{3.8}$$

▲

On remarque que le changement de variable ci-dessus n'est possible que si π est une permutation.

Lemme 3.14 ($U_{0\to1}$ *et les décompositions de Schmidt de* $|\zeta_0\rangle$ *et* $|\zeta_1\rangle$). Pour tout $\boldsymbol{v} \in \{0,1\}^k$ on a

$$U_{0\to1}|\xi(\boldsymbol{v})\rangle = \sqrt{2}^k \vec{\lambda}_{1,\pi^{-1}(\boldsymbol{v})}|\pi^{-1}(\boldsymbol{v})\rangle$$

où $|\xi(\boldsymbol{v})\rangle$ et $\vec{\lambda}_{1,\pi^{-1}(\boldsymbol{v})}$ sont tels qu'introduits aux remarques 3.12[61] et 3.13[61].

Preuve. De l'équation (3.4[58]), on récrit

$$(U_{0\to1} \otimes \mathbb{1}^{\mathrm{Bob}})|\zeta_0\rangle = |\zeta_1\rangle$$

et en substituant les expressions trouvées en (3.7[61]) et (3.8[61]) à $|\zeta_0\rangle$ et $|\zeta_1\rangle$:

$$(U_{0\to1} \otimes \mathbb{1}^{\mathrm{Bob}}) \sum_{\boldsymbol{v}} \frac{1}{\sqrt{2}^k}|\xi(\boldsymbol{v})\rangle|\boldsymbol{v}\rangle_\times = \sum_{\boldsymbol{v}\in\{0,1\}^k} \vec{\lambda}_{1,\pi^{-1}(\boldsymbol{v})}|\pi^{-1}(\boldsymbol{v})\rangle|\boldsymbol{v}\rangle_\times.$$

Il suffit d'utiliser le lemme 2.31[43] pour obtenir

$$U_{0\to1}|\xi(\boldsymbol{v})\rangle = \sqrt{2}^k \vec{\lambda}_{1,\pi^{-1}(\boldsymbol{v})}|\pi^{-1}(\boldsymbol{v})\rangle.$$

■

Le lemme 3.14[62] est la clef de notre inverseur. Si on est en mesure de produire l'état $|\xi(\boldsymbol{y})\rangle$ pour un $\boldsymbol{y}$ donné, alors la partie est gagnée en appliquant $U_{0\to1}$ à cet état. Cela nous mène au théorème suivant.

Théorème 3.15 (*validité de la réduction 3.11*[58]). Si l'adversaire $(\widetilde{C},U)$ de la réduction 3.11[58] est $(t(k),1)$-bon contre la condition liante du $\mathsf{BC_H}$ construit à la réduction 3.8[54], alors l'inverseur de π construit à la réduction 3.11[58] est $(t'(k),1)$-bon, pour $t'(k) \in O(t(k) + \|\pi_k\|_{\mathcal{U}} + k)$.

Preuve. Suivons pas à pas le circuit de la figure 3.7[60]:

$$|\boldsymbol{y}\rangle \quad \overset{C_0}{\longmapsto} \quad |\zeta_0\rangle|\boldsymbol{y}\rangle \tag{3.9}$$

$$
\begin{aligned}
&= \sum_{\boldsymbol{x}\in\{0,1\}^k} \vec{\lambda}_{0,\boldsymbol{x}} |\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle|\boldsymbol{y}\rangle && (3.10)\\
&\overset{\mathsf{C}\text{-}\sigma_z{}^{\otimes k}}{\longmapsto} \sum_{\boldsymbol{x}} (-1)^{y\odot\pi(x)} \vec{\lambda}_{0,\boldsymbol{x}} |\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle|\boldsymbol{y}\rangle \\
&\overset{\pi}{\longmapsto} \sum_{\boldsymbol{x}} (-1)^{y\odot\pi(x)} \vec{\lambda}_{0,\boldsymbol{x}} |\boldsymbol{x}\rangle|0^k\rangle|\boldsymbol{y}\rangle \\
&= |\xi(\boldsymbol{y})\rangle|0^k\rangle|\boldsymbol{y}\rangle && (3.11)\\
&\overset{U_{0\to 1}}{\longmapsto} \sqrt{2}^k \vec{\lambda}_{1,\pi^{-1}(\boldsymbol{y})} |\pi^{-1}(\boldsymbol{y})\rangle|0^k\rangle|\boldsymbol{y}\rangle.
\end{aligned}
$$

L'équation (3.9[62]) est obtenue de (3.3[58]), et la ligne (3.10[63]) par substitution du côté droit de (3.5[61]). L'application de $\mathsf{C}\text{-}\sigma_z{}^{\otimes k}$ permet d'introduire les phases nécessaires à la création de $|\xi(\boldsymbol{y})\rangle$. L'application de π *désintrique* les deux registres de droite du registre de gauche. Enfin (3.11[63]) découle de (3.6[61]), et il suffit d'invoquer le lemme 3.14[62] pour voir apparaître $\pi^{-1}(\boldsymbol{y})$ tel que promis. L'énoncé du théorème découle facilement de cette analyse. ■

Le traitement du cas imparfait se fait par l'introduction, dans le circuit de la réduction, de portes supplémentaires qui permettent de simplifier l'analyse.

Réduction 3.16 ($\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC_H}}$, *cas imparfait*). Soient $\widetilde{C}$ et U deux familles de circuits comme ceux de la réduction 3.11[58], mais cette fois l'attaque est imparfaite. Si

$$
\begin{aligned}
S_0 &\equiv ||\mathbb{P}_0|\zeta_0\rangle||^2 \\
\text{et} \qquad S_1 &\equiv ||\mathbb{P}_1|\zeta_1\rangle||^2
\end{aligned}
$$

sont les probabilités d'ouvrir respectivement $\mathsf{0}$ et $\mathsf{1}$ avec succès par cette attaque alors on a

$$S_0 + S_1 - 1 \geq s(k) \tag{3.12}$$

où $s(k) \notin \mathrm{negl}(k)$. L'inverseur est illustré à la figure 3.8[64]. ▲

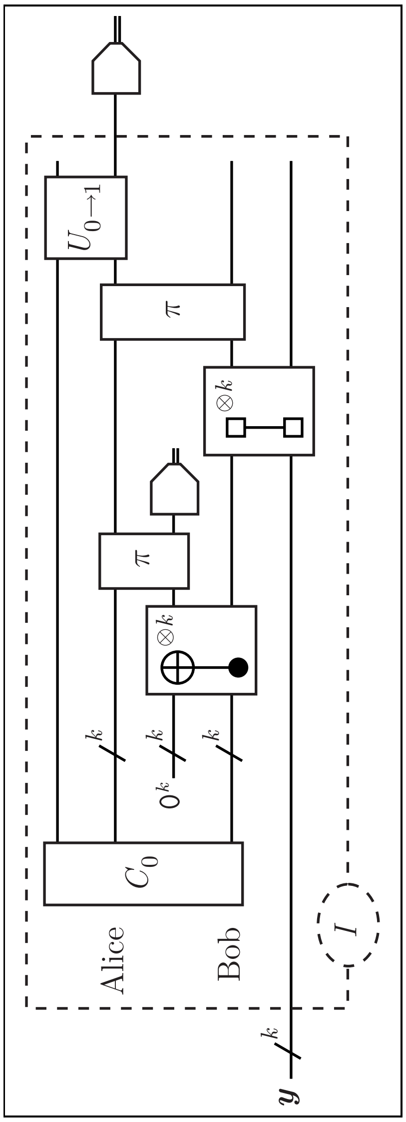


FIG. 3.8 – $\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC_H}}$, *cas imparfait*

Cette fois on doit accorder plus de généralité aux états $|\zeta_0\rangle$ et $|\zeta_1\rangle$.

Remarque 3.17 (*probabilités de succès des stratégies*). On peut poser

$$|\zeta_0\rangle \equiv \sum_{\boldsymbol{x}\in\{0,1\}^k} \sum_{\boldsymbol{z}\in\{0,1\}^k} \vec{\lambda}_{0,\boldsymbol{x},\boldsymbol{z}} |\boldsymbol{x}\rangle|\boldsymbol{z}\rangle, \tag{3.13}$$

d'où

$$\mathbb{P}_0|\zeta_0\rangle = \sum_{\boldsymbol{x}} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle \tag{3.14}$$

$$S_0 \equiv \|\mathbb{P}_0|\zeta_0\rangle\|^2 = \sum_{\boldsymbol{x}\in\{0,1\}^k} \|\vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})}\|^2, \tag{3.15}$$

de même que

$$|\zeta_1\rangle \equiv \sum_{\boldsymbol{x},\boldsymbol{z}} \vec{\lambda}_{1,\boldsymbol{x},\boldsymbol{z}} |\boldsymbol{x}\rangle|\boldsymbol{z}\rangle_\times$$

$$\mathbb{P}_1|\zeta_1\rangle = \sum_{\boldsymbol{x}} \vec{\lambda}_{1,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle_\times$$

$$S_1 \equiv \|\mathbb{P}_1|\zeta_1\rangle\|^2 = \sum_{\boldsymbol{x}\in\{0,1\}^k} \|\vec{\lambda}_{1,\boldsymbol{x},\pi(\boldsymbol{x})}\|^2.$$

▲

La remarque suivante est l'analogue de la remarque 3.12[61] faite pour le cas parfait.

Remarque 3.18 (*propriété de* $\mathbb{P}_0|\zeta_0\rangle$).

$$\mathbb{P}_0|\zeta_0\rangle = \sum_{\boldsymbol{x}\in\{0,1\}^k} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle|\pi(\boldsymbol{x})\rangle \tag{3.16}$$

$$= \sum_{\boldsymbol{x}} \sum_{\boldsymbol{v}\in\{0,1\}^k} \frac{(-1)^{\boldsymbol{v}\odot\pi(\boldsymbol{x})}}{\sqrt{2}^k} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle|\boldsymbol{v}\rangle_\times \tag{3.17}$$

$$\boxed{|\xi(\boldsymbol{v})\rangle \equiv \sum_{\boldsymbol{x}\in\{0,1\}^k} \frac{(-1)^{\boldsymbol{v}\odot\pi(\boldsymbol{x})}}{\sqrt{S_0}} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle} \tag{3.18}$$

$$= \sum_{\boldsymbol{v}} \frac{\sqrt{S_0}}{\sqrt{2}^k} |\xi(\boldsymbol{v})\rangle|\boldsymbol{v}\rangle_\times. \tag{3.19}$$

La ligne (3.16[65]) est identique à la ligne (3.14[65]); la ligne (3.17[65]) s'obtient à la l'aide de la formule de changement de base (2.14[41]); il est facile de vérifier que $|\xi(\boldsymbol{v})\rangle$ est bien de norme 1 au moyen de la ligne (3.15[65]). De la ligne (3.19[65]) on conclut que $|\xi(\boldsymbol{v})\rangle|\boldsymbol{v}\rangle_\times$ s'obtient en appliquant le projecteur $\mathbb{1}\otimes|\boldsymbol{v}\rangle_\times\langle\boldsymbol{v}|$ au vecteur $\mathbb{P}_0|\zeta_0\rangle$ et en renormalisant, ce qui s'exprime comme ceci:

$$|\xi(\boldsymbol{v})\rangle|\boldsymbol{v}\rangle_\times \quad = \quad \frac{\sqrt{2}^k}{\sqrt{S_0}}\;(\mathbb{1}\otimes|\boldsymbol{v}\rangle_\times\langle\boldsymbol{v}|)\;\mathbb{P}_0\;|\zeta_0\rangle.$$

▲

Nous sommes maintenant prêts à établir le théorème central de ce chapitre.

Théorème 3.19 (*validité de la réduction 3.16*[63]). Si l'adversaire $(\widetilde{C},U)$ de la réduction 3.16[63] est $(t(k),s(k))$-bon contre la condition liante du $\mathsf{BC_H}$ construit à la réduction 3.8[54], alors l'inverseur de π construit à la réduction 3.16[63] est $(t'(k),s'(k))$-bon, pour $t'(k)\in O(t(k)+\|\pi_k\|_{\mathcal{U}}+k)$ et pour $s'(k)\in\Omega(s(k)^2)$.

Preuve. Suivons le circuit de la figure 3.8[64] porte par porte:

$$\begin{aligned} |\vdash\rangle|\boldsymbol{y}\rangle \quad &\overset{C_0}{\longmapsto} \quad |\zeta_0\rangle|\boldsymbol{y}\rangle && (3.20)\\ &= \quad \sum_{\boldsymbol{x}\in\{0,1\}^k}\;\sum_{\boldsymbol{z}\in\{0,1\}^k}\vec{\lambda}_{0,\boldsymbol{x},\boldsymbol{z}}|\boldsymbol{x}\rangle|\boldsymbol{z}\rangle|\boldsymbol{y}\rangle. && (3.21)\end{aligned}$$

La ligne (3.20[66]) vient de (3.3[58]) qui est toujours valide dans le cas imparfait; l'équation (3.21[66]) découle de la ligne (3.13[65]). À partir d'ici nous insérons un registre supplémentaire entre les registres $|\boldsymbol{x}\rangle^{\text{Alice}}$ et $|\boldsymbol{z}\rangle^{\text{Bob}}$:

$$\begin{aligned} &= \quad \sum_{\boldsymbol{x},\boldsymbol{z}}\vec{\lambda}_{0,\boldsymbol{x},\boldsymbol{z}}|\boldsymbol{x}\rangle|0^k\rangle|\boldsymbol{z}\rangle|\boldsymbol{y}\rangle && (3.22)\\ &\overset{\mathsf{C\text{-}NOT}^{\otimes k}}{\longmapsto} \quad \sum_{\boldsymbol{x},\boldsymbol{z}}\vec{\lambda}_{0,\boldsymbol{x},\boldsymbol{z}}|\boldsymbol{x}\rangle|\boldsymbol{z}\rangle|\boldsymbol{z}\rangle|\boldsymbol{y}\rangle\\ &\overset{\pi}{\longmapsto} \quad \sum_{\boldsymbol{x},\boldsymbol{z}}\vec{\lambda}_{0,\boldsymbol{x},\boldsymbol{z}}|\boldsymbol{x}\rangle|\boldsymbol{z}\oplus\pi(\boldsymbol{x})\rangle|\boldsymbol{z}\rangle|\boldsymbol{y}\rangle.\end{aligned}$$

Avec de la chance, la mesure effectuée au milieu du circuit de la figure 3.8[64] projette notre registre supplémentaire sur le vecteur $|0^k\rangle$. Nous conservons implicitement la probabilité de cet événement dans la suite du calcul *en ne renormalisant pas nos états successifs*. En effet, nous n'avons qu'à calculer la norme au carré d'un état pour connaître la probabilité avec laquelle une mesure a pu le mettre au monde. Nous poursuivons donc en appliquant le projecteur $|0^k\rangle\langle 0^k|$ au registre supplémentaire. On remarque que dans l'espace de cette projection, on a que $\boldsymbol{z} = \pi(\boldsymbol{x})$:

$$\overset{|0^k\rangle\langle 0^k|}{\longmapsto} \quad \sum_{\boldsymbol{x}} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle |0^k\rangle |\pi(\boldsymbol{x})\rangle |\boldsymbol{y}\rangle.$$

Nous pouvons maintenant oublier le registre inséré en (3.22[66]):

$$\begin{aligned} &= \sum_{\boldsymbol{x}} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle |\pi(\boldsymbol{x})\rangle |\boldsymbol{y}\rangle \\ &= \mathbb{P}_0 |\zeta_0\rangle \otimes |\boldsymbol{y}\rangle. \end{aligned} \tag{3.23}$$

La ligne (3.23[67]) provient de (3.14[65]). À partir de maintenant, le circuit est identique au circuit du cas parfait:

$$\begin{aligned} &\overset{\mathsf{C}\text{-}\sigma_z{}^{\otimes k}}{\longmapsto} \quad \sum_{\boldsymbol{x}} (-1)^{\boldsymbol{y} \odot \pi(\boldsymbol{x})} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle |\pi(\boldsymbol{x})\rangle |\boldsymbol{y}\rangle \\ &\overset{\pi}{\longmapsto} \quad \sum_{\boldsymbol{x}} (-1)^{\boldsymbol{y} \odot \pi(\boldsymbol{x})} \vec{\lambda}_{0,\boldsymbol{x},\pi(\boldsymbol{x})} |\boldsymbol{x}\rangle |0^k\rangle |\boldsymbol{y}\rangle \\ &= \quad \sqrt{S_0} |\xi(\boldsymbol{y})\rangle |0^k\rangle |\boldsymbol{y}\rangle \qquad (3.24) \\ &\overset{U_{0\to 1}}{\longmapsto} \quad \sqrt{S_0} \;\; (U_{0\to 1} |\xi(\boldsymbol{y})\rangle) \otimes |0^k\rangle |\boldsymbol{y}\rangle \\ &\overset{\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}}{\longmapsto} \quad \sqrt{S_0} \left(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})} U_{0\to 1} |\xi(\boldsymbol{y})\rangle \right) \otimes |0^k\rangle |\boldsymbol{y}\rangle \qquad (3.25) \end{aligned}$$

où

$$\mathbb{P}_{\pi^{-1}(\boldsymbol{y})} \equiv \mathbb{1}^{\mathrm{Etc}} \otimes |\pi^{-1}(\boldsymbol{y})\rangle^{\mathrm{Alice}} \langle \pi^{-1}(\boldsymbol{y})|.$$

La ligne (3.24[67]) découle de (3.18[65]); les deux lignes suivantes sont triviales. Le projecteur $\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}$ est utilisé en dernier lieu de telle sorte que la norme au carré de l'état de la ligne (3.25[67]) nous donne la probabilité de succès de l'inverseur pour un certain $\boldsymbol{y}$ fixé, ce que nous notons $p_{\boldsymbol{y}}$. Calculons cette probabilité:

$$
\begin{aligned}
p_{\boldsymbol{y}} &= \|\sqrt{S_0}\ \ \big(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}\, U_{0\to 1}|\xi(\boldsymbol{y})\rangle\big)\ \otimes\ |0^k\rangle|\boldsymbol{y}\rangle\|^2 \\
&= \|\sqrt{S_0}\ \ \big(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}\, U_{0\to 1}|\xi(\boldsymbol{y})\rangle\big)\ \otimes\ |\boldsymbol{y}\rangle_\times\|^2 \\
&= \|\sqrt{S_0}\ \ \big(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}\, U_{0\to 1}\ \otimes\ \mathbb{1}\big)\ \ |\xi(\boldsymbol{y})\rangle|\boldsymbol{y}\rangle_\times\|^2 \\
&= \left\|\frac{\sqrt{S_0}\sqrt{2}^k}{\sqrt{S_0}}\ \ \big(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}\, U_{0\to 1}\ \otimes\ |\boldsymbol{y}\rangle_\times\langle\boldsymbol{y}|\big)\ \ \mathbb{P}_0\ \ |\zeta_0\rangle\right\|^2. \qquad (3.26)
\end{aligned}
$$

La ligne (3.26[68]) est obtenue grâce à (3.20[66]). Comme la probabilité de succès p de l'inverseur est calculée pour $\boldsymbol{y}$ choisi uniformément au hasard dans $\{0,1\}^k$, nous avons:

$$
\begin{aligned}
p &= \sum_{\boldsymbol{y}\in\{0,1\}^k} \frac{1}{2^k} p_{\boldsymbol{y}} \\
&= \sum_{\boldsymbol{y}} \frac{1}{2^k}\|\sqrt{2}^k\ \ \big(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}\, U_{0\to 1}\ \otimes\ |\boldsymbol{y}\rangle_\times\langle\boldsymbol{y}|\big)\ \ \mathbb{P}_0\ \ |\zeta_0\rangle\|^2 \\
&= \sum_{\boldsymbol{y}} \|\big(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}\, U_{0\to 1}\ \otimes\ |\boldsymbol{y}\rangle_\times\langle\boldsymbol{y}|\big)\ \ \mathbb{P}_0\ \ |\zeta_0\rangle\|^2 \\
&= \|\sum_{\boldsymbol{y}} \big(\mathbb{P}_{\pi^{-1}(\boldsymbol{y})}\, U_{0\to 1}\ \otimes\ |\boldsymbol{y}\rangle_\times\langle\boldsymbol{y}|\big)\ \ \mathbb{P}_0\ \ |\zeta_0\rangle\|^2 \qquad (3.27) \\
&= \left\|\left(\sum_{\boldsymbol{y}} \mathbb{P}_{\pi^{-1}(\boldsymbol{y})} \otimes |\boldsymbol{y}\rangle_\times\langle\boldsymbol{y}|\right)(U_{0\to 1}\otimes\mathbb{1})\ \mathbb{P}_0\ |\zeta_0\rangle\right\|^2 \\
&\geq \|\mathbb{P}_1\ \ (U_{0\to 1}\ \otimes\ \mathbb{1})\ \ \mathbb{P}_0\ \ |\zeta_0\rangle\|^2. \qquad (3.28)
\end{aligned}
$$

Pour obtenir la ligne (3.27[68]), il est permis de sortir la norme au carré de la sommation en invoquant la proposition 2.22[32] : les termes de la somme sont orthogonaux deux à deux, parce que les membres de la famille de projecteurs

$$\{\ \mathbb{P}_{\pi^{-1}(\boldsymbol{y})} \otimes |\boldsymbol{y}\rangle_\times\langle\boldsymbol{y}|\ \}_{\boldsymbol{y}\in\{0,1\}^k}$$

sont eux-mêmes orthogonaux deux à deux. La ligne (3.28[68]) est due à la définition de $\mathbb{P}_1$ donnée à la réduction 3.8[54] (nous devons utiliser un signe d'inégalité par la proposition 2.19[31], puisque $\mathbb{P}_1$ comporte un projecteur $|1\rangle\langle 1|$ sur le registre contenant l'annonce du bit à l'ouverture). Le reste de l'analyse consiste à borner inférieurement p par une fonction de S_0 et S_1:

$$\begin{aligned}
\sqrt{p} &= \|\mathbb{P}_1\ U_{0\to 1}\ \mathbb{P}_0\ |\zeta_0\rangle\| \\
&\equiv \|\mathbb{P}_1\ U_{0\to 1}\ (\mathbb{1} - \mathbb{P}_0^{\perp})\ |\zeta_0\rangle\| && (3.29)\\
&= \|\mathbb{P}_1 U_{0\to 1}|\zeta_0\rangle \ - \ \mathbb{P}_1 U_{0\to 1}\mathbb{P}_0^{\perp}|\zeta_0\rangle\| \\
&= \|\mathbb{P}_1|\zeta_1\rangle \ - \ \mathbb{P}_1 U_{0\to 1}\mathbb{P}_0^{\perp}|\zeta_0\rangle\| && (3.30)\\
&\geq \|\mathbb{P}_1|\zeta_1\rangle\| \ - \ \|\mathbb{P}_1 U_{0\to 1}\mathbb{P}_0^{\perp}|\zeta_0\rangle\| && (3.31)\\
&\geq \|\mathbb{P}_1|\zeta_1\rangle\| \ - \ \|\mathbb{P}_0^{\perp}|\zeta_0\rangle\| && (3.32)\\
&= \sqrt{S_1} \ - \ \sqrt{1 - S_0}. && (3.33)
\end{aligned}$$

La ligne (3.30[69]) est donnée par (3.4[58]); la ligne (3.31[69]) est obtenue à l'aide de l'inégalité du triangle; on invoque la proposition 2.19[31] pour la ligne (3.32[69]); et la ligne (3.33[69]) découle des définitions de S_0 et S_1 à la remarque 3.17[65] et celle de $\mathbb{P}_0^{\perp}$ à la ligne (3.29[69]). La ligne suivante (3.34[69]) n'est permise que si l'expression (3.33[69]) est positive, ce qui est le cas puisque $S_0 + S_1 \geq 1$ par l'hypothèse émise à la ligne (3.12[63]):

$$p \ \geq \ \left(\sqrt{S_1} \ - \ \sqrt{1 - S_0}\right)^2. \qquad (3.34)$$

Il suffit d'une analyse de calcul différentiel élémentaire pour arriver à l'énoncé du théorème à partir de (3.34[69]). ■

Chapitre 4

Mise en gage quantique d'une chaîne de bits

Au prochain chapitre, nous aurons besoin de mettre en gage plusieurs bits à la fois. Afin de mettre en gage une chaîne de m bits, il semble naturel de soumettre chacun des bits à une mise en gage individuelle, en prenant soin de procéder de façon indépendante sur chaque bit lorsque des choix aléatoires doivent être faits, et c'est ce que nous allons faire. Le but du présent chapitre est d'analyser de quelle façon dépend la sécurité d'une telle mise en gage de chaîne de bits sur les mises en gage inconditionnellement camouflantes sous-jacentes. Nous en profitons aussi pour introduire quelques définitions.

Notre approche sera moins formelle qu'elle ne l'a été jusqu'à maintenant, mais nous donnons suffisamment de détails pour aborder le chapitre 5 en toute tranquillité.

4.1 Mise en gage de deux bits

Nous considérons d'abord un cas simple. Tous les arguments auxquels nous devons faire appel dans les autres cas peuvent être mis en scène lorsque seulement deux bits sont mis en gage. Les preuves s'en trouvent simplifiées et l'argumentation plus facile à suivre.

Notre but est de mettre en gage 2 bits étant donnée une primitive permettant d'en n'engager qu'un seul. Nous adoptons le sigle $2\mathsf{BC_H}$ pour la primitive de mise en gage inconditionnellement camouflante de deux bits. Formellement, si $(C,\mathbb{Q})$ est une paire de famille de circuits quantiques qui implantent un $\mathsf{BC_H}$ parfaitement camouflant et non interactif, tel que décrit aux définitions 3.2[51] et 3.4[52] et à la figure 3.3[51], alors le protocole honnête $2\mathsf{BC_H}$ consiste à s'engager à chacun des deux bits de façon indépendante à l'aide du circuit C. La mesure

$$[\ \mathbb{Q}_0 \otimes \mathbb{Q}_0,\ \mathbb{Q}_0 \otimes \mathbb{Q}_1,\ \mathbb{Q}_1 \otimes \mathbb{Q}_0,\ \mathbb{Q}_1 \otimes \mathbb{Q}_1,\ \mathbb{1} - \sum_{b_1,b_2\, \in \{0,1\}} \mathbb{Q}_{b_1} \otimes \mathbb{Q}_{b_2}\ ]$$

sera le test d'ouverture du $2\mathsf{BC_H}$. Il est possible de n'ouvrir qu'une seule des deux positions. Par exemple, la mesure

$$[\ \mathbb{Q}_0 \otimes \mathbb{1},\ \mathbb{Q}_1 \otimes \mathbb{1},\ \mathbb{1} \otimes \mathbb{1} - \mathbb{Q}_0 \otimes \mathbb{1} - \mathbb{Q}_1 \otimes \mathbb{1}\ ]$$

permet d'ouvrir le bit en première position. Nous prenons soin de définir formellement l'adversaire à la condition liante de $2\mathsf{BC_H}$.

Définition 4.1 (*mise en gage quantique de deux bits: adversaire à la condition liante*). Un *adversaire à la condition liante* d'une mise en gage quantique sur deux bits telle que décrite au paragraphe précédent est une paire de familles de circuits quantiques

$$\widetilde{C} = \{\widetilde{C}_k\}_{k>0},\ U = \{U_k\}_{k>0}$$

qui répondent à des spécifications semblables à celles de la figure 3.4[53], sauf que c'est maintenant une chaîne $\boldsymbol{b}$ de deux bits qui entre dans le circuit de l'attaque. Un tel adversaire est $(t(k),s(k))$-bon si

$$\|\widetilde{C}\|_{\mathcal{U}} + \|U\|_{\mathcal{U}} \in O(t(k)),$$

et si

$$\|(\mathbb{Q}_0 \otimes \mathbb{Q}_0)|\zeta_{00}\rangle\|^2 + \|(\mathbb{Q}_0 \otimes \mathbb{Q}_1)|\zeta_{01}\rangle\|^2 + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_0)|\zeta_{10}\rangle\|^2 + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_1)|\zeta_{11}\rangle\|^2 - 1 \geq s(k). \quad (4.1)$$

L'entier k sert de paramètre de sécurité. On dira que les quatre états $|\zeta_{00}\rangle$, $|\zeta_{01}\rangle$, $|\zeta_{10}\rangle$ et $|\zeta_{11}\rangle$ *incarnent* cette attaque. Si

$$\|(\mathbb{Q}_0 \otimes \mathbb{Q}_0)|\zeta_{00}\rangle\|^2 + \|(\mathbb{Q}_0 \otimes \mathbb{Q}_1)|\zeta_{01}\rangle\|^2 + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_0)|\zeta_{10}\rangle\|^2 + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_1)|\zeta_{11}\rangle\|^2 = 4,$$

alors on dira que l'adversaire est *parfait*. ▲

Comme d'habitude, le paramètre de sécurité k sert implicitement d'indice aux familles de circuits C, $\mathbb{Q}$, $\widetilde{C}$ et U, de même qu'aux états $|\zeta_{\boldsymbol{b}}\rangle$. À l'instar de la remarque 3.6[53], on peut réaliser un "adversaire" $(\|C\|_{\mathcal{U}},0)$-bon en s'engageant honnêtement à une chaîne quelconque.

La réduction $\mathcal{A}_{\mathsf{BC_H}} \leq_\exists \mathcal{A}_{\mathsf{2BC_H}}$ est nécessaire pour démontrer la sécurité du côté calculatoire de ce $\mathsf{2BC_H}$. Comme la notation l'indique, nous devrons nous contenter d'une réduction non uniforme. Et comme l'énoncé du théorème suivant le signale, notre réduction n'est valide que pour une certaine classe d'adversaires $\mathcal{A}_{\mathsf{2BC_H}}$. En somme, notre résultat est perfectible en ce qui a trait à la probabilité de succès des adversaires considérés.

Théorème 4.2 ($\mathcal{A}_{\mathsf{BC_H}} \leq_\exists \mathcal{A}_{\mathsf{2BC_H}}$, *lorsque* $\mathcal{A}_{\mathsf{2BC_H}}$ *est* $(t(k),\ 1+\epsilon(k))$*-bon*).

Soient $|\zeta_{00}\rangle$, $|\zeta_{01}\rangle$, $|\zeta_{10}\rangle$ et $|\zeta_{11}\rangle$ quatre états incarnant une attaque $(t(k),1+\epsilon(k))$-bonne sur $2\mathsf{BC_H}$, c'est-à-dire:

$$\begin{aligned}\|(\mathbb{Q}_0 \otimes \mathbb{Q}_0)|\zeta_{00}\rangle\|^2 + \|(\mathbb{Q}_0 \otimes \mathbb{Q}_1)|\zeta_{01}\rangle\|^2 \\ + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_0)|\zeta_{10}\rangle\|^2 + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_1)|\zeta_{11}\rangle\|^2 \geq 2 + \epsilon(k). \quad (4.2)\end{aligned}$$

Alors il existe une attaque $(t(k),\frac{\epsilon(k)}{2})$-bonne sur $\mathsf{BC_H}$.

Preuve. De l'équation (4.2[73]) on conclut de deux choses l'une:

$$\|(\mathbb{Q}_0 \otimes \mathbb{Q}_0)|\zeta_{00}\rangle\|^2 + \|(\mathbb{Q}_0 \otimes \mathbb{Q}_1)|\zeta_{01}\rangle\|^2 \geq 1 + \frac{\epsilon(k)}{2} \quad (4.3)$$

ou

$$\|(\mathbb{Q}_1 \otimes \mathbb{Q}_0)|\zeta_{10}\rangle\|^2 + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_1)|\zeta_{11}\rangle\|^2 \geq 1 + \frac{\epsilon(k)}{2}. \quad (4.4)$$

Dans le cas (4.3[73]), les états $|\zeta_{00}\rangle$ et $|\zeta_{01}\rangle$ incarnent une attaque $(t(k),\frac{\epsilon(k)}{2})$-bonne sur la mise en gage du bit de droite. En effet, de (4.3[73]) et des inégalités

$$\begin{aligned}\|(\mathbb{1} \otimes \mathbb{Q}_0)|\zeta_{00}\rangle\|^2 &\geq \|(\mathbb{Q}_0 \otimes \mathbb{Q}_0)|\zeta_{00}\rangle\|^2 \\ \|(\mathbb{1} \otimes \mathbb{Q}_1)|\zeta_{01}\rangle\|^2 &\geq \|(\mathbb{Q}_0 \otimes \mathbb{Q}_1)|\zeta_{01}\rangle\|^2,\end{aligned}$$

on tire

$$\|(\mathbb{1} \otimes \mathbb{Q}_0)|\zeta_{00}\rangle\|^2 + \|(\mathbb{1} \otimes \mathbb{Q}_1)|\zeta_{01}\rangle\|^2 - 1 \geq \frac{\epsilon(k)}{2}.$$

Le raisonnement est semblable dans le cas (4.4[73]) et nous donne une attaque sur la mise en gage du bit de gauche. ∎

À propos du théorème 4.2[72], il est important de remarquer deux choses. D'une part, l'argument utilisé est purement combinatoire et ne donne pas une construction explicite de l'adversaire $\mathcal{A}_{\mathsf{BC_H}}$. C'est pour cette raison que la réduction est non uniforme. Nous aurons de nouveau aurons recours à ce type d'argument combinatoire au chapitre 5. D'autre part, puisque les circuits $\widetilde{C}$ et U qui servent à construire les états $|\zeta_{00}\rangle$, $|\zeta_{01}\rangle$, $|\zeta_{10}\rangle$ et $|\zeta_{11}\rangle$ sont connus de l'attaquant, rien n'empêche celui-ci de les utiliser dans un précalcul destiné à déterminer lequel des cas (4.3[73]) ou (4.4[73]) s'avère. Dans un tel scénario, la réduction devient constructive, mais il semble difficile de faire une analyse du prix calculatoire à payer pour la réaliser. Ces problèmes d'uniformisation des réductions seront revus au chapitre 6 (problème P9[125]).

Le théorème 4.2[72] ne nous donne pas une réduction pour tous les adversaires $\mathcal{A}_{2\mathsf{BC}_\mathsf{H}}$ $(t(k),s(k))$-bons, mais seulement pour ceux qui sont tels que $s(k) \geq 1+\epsilon(k)$. Mince consolation, il est possible de troquer cette restriction pour une autre. Par exemple, si l'on suppose que le résultat de l'expérience aléatoire qui consiste à ouvrir un des deux bits est indépendant du succès de l'ouverture de l'autre position, alors on peut exhiber une réduction (non uniforme) pour tous les adversaires $(t(k),s(k))$-bons non triviaux, c'est-à-dire aussitôt que $s(k)$ est non négligeable en k. Une telle restriction serait valide par exemple si l'attaquant s'en prend à chaque bit de façon indépendante et que les états $|\zeta_{b_1,b_2}\rangle$ qui incarnent l'attaque sont, en fait, des produits tensoriels d'états sur chacune des deux positions. Il va s'en dire qu'une telle restriction est drastique et qu'elle appauvrit considérablement la classe des adversaires admissibles. Pour cette raison, l'intérêt de ces considérations est mitigé, et nous passons outre.

4.2 Mise en gage de m bits

Il est facile de généraliser l'approche de la section précédente à la mise en gage d'une chaîne de m bits, pour tout $m \geq 1$, primitive que nous noterons $m\mathsf{BC}_\mathsf{H}$.

Définition 4.3 (*mise en gage quantique de m bits: adversaire à la condition liante*). Un *adversaire à la condition liante* d'une mise en gage quantique sur m

bits est une paire de familles de circuits quantiques

$$\widetilde{C} = \{\widetilde{C}_k\}_{k>0},\ U = \{U_k\}_{k>0}$$

qui se conforment à des spécifications semblables à celles de la figure 3.4[53], sauf que c'est maintenant une chaîne $\boldsymbol{b}$ de m bits qui entre dans le circuit de l'attaque. Un tel adversaire est $(t(k),s(k))$-bon si

$$\|\widetilde{C}\|_{\mathcal{U}} + \|U\|_{\mathcal{U}} \in O(t(k)),$$

et si

$$\sum_{\boldsymbol{b}\in\{\mathtt{0},\mathtt{1}\}^m} \|(\mathbb{Q}_{\boldsymbol{b}[1]} \otimes \cdots \otimes \mathbb{Q}_{\boldsymbol{b}[m]})|\zeta_{\boldsymbol{b}}\rangle\|^2 - 1 \geq s(k). \tag{4.5}$$

L'entier k sert de paramètre de sécurité. On dira que les 2^m états

$$\{|\zeta_{\boldsymbol{b}}\rangle\ :\ \boldsymbol{b} \in \{\mathtt{0},\mathtt{1}\}^m\}$$

incarnent cette attaque. Si

$$\sum_{\boldsymbol{b}} \|(\mathbb{Q}_{\boldsymbol{b}[1]} \otimes \cdots \otimes \mathbb{Q}_{\boldsymbol{b}[m]})|\zeta_{\boldsymbol{b}}\rangle\|^2 = 2^m,$$

alors on dira que l'adversaire est *parfait*. ▲

Le théorème 4.2[72] est généralisé à la proposition suivante. La preuve de cette proposition est un exercice facile à la lumière de celle du théorème 4.2[72].

Proposition 4.4 ($\mathcal{A}_{\mathsf{BC_H}} \leq_{\exists} \mathcal{A}_{m\mathsf{BC_H}}$, *lorsque* $\mathcal{A}_{m\mathsf{BC_H}}$ *est* $(t(k),\ 2^{m-1}-1+\epsilon(k))$*-bon*). Soient $\{|\zeta_{\boldsymbol{b}}\rangle\}_{\boldsymbol{b}\in\{\mathtt{0},\mathtt{1}\}^m}$ la famille des 2^m états incarnant une attaque $(t(k),2^{m-1}-1+\epsilon(k))$-bonne sur un $m\mathsf{BC_H}$ construit par la concaténation de m $\mathsf{BC_H}$, c'est-à-dire:

$$\sum_{\boldsymbol{b}\in\{\mathtt{0},\mathtt{1}\}^m} \|(\mathbb{Q}_{\boldsymbol{b}[1]} \otimes \cdots \otimes \mathbb{Q}_{\boldsymbol{b}[m]})|\zeta_{\boldsymbol{b}}\rangle\|^2 \geq 2^{m-1} + \epsilon(k). \tag{4.6}$$

Alors il existe une attaque $(t(k),\frac{\epsilon(k)}{2^{m-1}})$-bonne sur $\mathsf{BC_H}$. ▲

La définition 4.3[74] et la proposition 4.4[75] vont de soi tant que m est considéré comme une constante par rapport au paramètre de sécurité k. Mais la question de la qualité d'un adversaire à la condition liante d'une mise gage d'une chaîne de bits doit être envisagée avec précaution lorsque m et k sont liés de façon polynômiale, ce que souligne la remarque suivante.

Remarque 4.5 (*mise en gage de m bits et paramètre de sécurité k*). Si $m \notin \mathrm{polylog}(k)$, par exemple si $m = k$, alors il est possible que pour tout $\boldsymbol{b} \in \{0,1\}^m$ on ait

$$\|(\mathbb{Q}_{\boldsymbol{b}[1]} \otimes \cdots \otimes \mathbb{Q}_{\boldsymbol{b}[m]})|\zeta_{\boldsymbol{b}}\rangle\|^2 \in \mathrm{negl}(k)$$

et que la ligne (4.5[75]) soit néanmoins satisfaite. Dans un tel cas, l'attaque incarnée par les 2^m états $|\zeta_{\boldsymbol{b}}\rangle$ serait statistiquement indistinguable d'une mise en gage honnête.

Pour que la ligne (4.5[75]) ait quelque valeur cryptographique, toujours dans le cas où $m \notin \mathrm{polylog}(k)$, il est suffisant de s'assurer que l'avantage $s(k)$ soit réparti sur un nombre d'états $|\zeta_{\boldsymbol{b}}\rangle$ qui soit dans $\mathrm{poly}(m)$. ▲

Bien que les définitions 4.1[71] ou 4.3[74] soient des généralisations naturelles de la définition 3.5[53], il est possible de généraliser encore un peu. Par exemple l'attaquant à $2\mathsf{BC}_\mathsf{H}$ pourrait s'en prendre à un seul des deux bits plutôt qu'aux deux, ou encore à un prédicat des deux bits. Cette nouvelle généralisation n'est pas vaine car elle entrera en action au chapitre 5. En voici une définition formelle:

Définition 4.6 (*mise en gage quantique de m bits: adversaire à la condition liante généralisé*). Soit $f : \{0,1\}^m \longrightarrow \{0,1\}^\ell$ une fonction surjective de m bits à ℓ bits, où $1 \leq \ell \leq m$. Un *adversaire à la condition liante sur f* d'une mise en gage quantique de m bits — ou plus simplement un *f-adversaire* — est une paire de familles de circuits quantiques

$$\widetilde{C} = \{\widetilde{C}_k\}_{k>0},\ U = \{U_k\}_{k>0}$$

qui répondent à des spécifications semblables à celles de la figure 3.4[53], sauf que c'est maintenant une chaîne $\boldsymbol{d}$ de ℓ bits qui entre dans le circuit de l'attaque. Un tel f-adversaire est $(t(k),s(k))$-bon si

$$\|\widetilde{C}\|_{\mathcal{U}} + \|U\|_{\mathcal{U}} \in O(t(k)),$$

$$\sum_{\boldsymbol{d}\in\{0,1\}^\ell} \|(\sum_{\boldsymbol{b}\in f^{-1}(\boldsymbol{d})} \mathbb{Q}_{\boldsymbol{b}[1]} \otimes \cdots \otimes \mathbb{Q}_{\boldsymbol{b}[m]})|\zeta_{\boldsymbol{d}}\rangle\|^2 \;-\; 1 \;\;\geq\;\; s(k). \tag{4.7}$$

L'entier k sert de paramètre de sécurité. On dira que les 2^ℓ états

$$\{|\zeta_{\boldsymbol{d}}\rangle \;:\; \boldsymbol{d} \in \{0,1\}^\ell\}$$

incarnent cette f-attaque. Si

$$\sum_{\boldsymbol{d}\in\{0,1\}^\ell} \|(\sum_{\boldsymbol{b}\in f^{-1}(\boldsymbol{d})} \mathbb{Q}_{\boldsymbol{b}[1]} \otimes \cdots \otimes \mathbb{Q}_{\boldsymbol{b}[m]})|\zeta_{\boldsymbol{d}}\rangle\|^2 = 2^\ell,$$

alors on dira que cet f-adversaire est *parfait*. ▲

La notation $\mathcal{A}^\ell_{m\mathsf{BC_H}}$ désignera un f-adversaire à $m\mathsf{BC_H}$ pour $f : \{0,1\}^m \to \{0,1\}^\ell$. Il est facile de voir que l'adversaire de la définition 3.5[53] est un f-adversaire pour la fonction *identité* sur $\{0,1\}$. De la même façon, celui de la définition 4.1[71] est un f-adversaire pour la fonction *identité* sur $\{0,1\}^2$.

Lorsque $m \notin \text{polylog}(k)$, la définition 4.6[76] apporte une réponse à la remarque 4.5[76]:

Remarque 4.7 ($\mathcal{A}^\ell_{m\mathsf{BC_H}}$ *et paramètre de sécurité* k). À la lumière de la remarque 4.5[76], si $m \notin \text{polylog}(k)$, alors les adversaires $\mathcal{A}^\ell_{m\mathsf{BC_H}}$ intéressants — c'est-à-dire susceptibles de procurer une réduction depuis $\mathcal{A}_{\mathsf{BC_H}}$ — sont ceux pour lesquels $\ell \in \text{polylog}(m)$. ▲

Lorsque $m = 2$ et $\ell = 1$ nous relevons les trois cas particuliers suivants qui joueront un rôle à la section 5.3.1[85]. Pour

$$f_1 \;:\; (b_1,b_2) \longmapsto b_1$$

on obtient un *attaquant à la condition liante sur le premier bit* et la sommation de la ligne (4.7[77]) s'écrit:

$$\|(\mathbb{Q}_0 \otimes \mathbb{Q}_0 + \mathbb{Q}_0 \otimes \mathbb{Q}_1)|\zeta_0\rangle\|^2 + \|(\mathbb{Q}_1 \otimes \mathbb{Q}_0 + \mathbb{Q}_1 \otimes \mathbb{Q}_1)|\zeta_1\rangle\|^2 =$$
$$\|\mathbb{Q}_0 \otimes \mathbb{Q}_0|\zeta_0\rangle\|^2 + \|\mathbb{Q}_0 \otimes \mathbb{Q}_1|\zeta_0\rangle\|^2 + \|\mathbb{Q}_1 \otimes \mathbb{Q}_0|\zeta_1\rangle\|^2 + \|\mathbb{Q}_1 \otimes \mathbb{Q}_1|\zeta_1\rangle\|^2 \quad (4.8)$$

en invoquant la proposition 2.22[32]; pour

$$f_2 \;:\; (b_1,b_2) \longmapsto b_2$$

on obtient un *attaquant à la condition liante sur le deuxième bit* et la sommation de la ligne (4.7[77]) s'écrit:

$$\|\mathbb{Q}_0 \otimes \mathbb{Q}_0|\zeta_0\rangle\|^2 + \|\mathbb{Q}_1 \otimes \mathbb{Q}_0|\zeta_0\rangle\|^2 + \|\mathbb{Q}_0 \otimes \mathbb{Q}_1|\zeta_1\rangle\|^2 + \|\mathbb{Q}_1 \otimes \mathbb{Q}_1|\zeta_1\rangle\|^2; \quad (4.9)$$

et pour

$$f_3 \;:\; (b_1,b_2) \longmapsto b_1 \oplus b_2$$

on obtient un *attaquant à la condition liante sur le ou exclusif de deux bits* et la sommation s'écrit:

$$\|\mathbb{Q}_0 \otimes \mathbb{Q}_0|\zeta_0\rangle\|^2 + \|\mathbb{Q}_1 \otimes \mathbb{Q}_1|\zeta_0\rangle\|^2 + \|\mathbb{Q}_0 \otimes \mathbb{Q}_1|\zeta_1\rangle\|^2 + \|\mathbb{Q}_1 \otimes \mathbb{Q}_0|\zeta_1\rangle\|^2. \quad (4.10)$$

Il est facile sinon trivial de réduire un attaquant à la condition liante de BC_H à un f_1-attaquant ou à un f_2-attaquant sur $2\mathsf{BC}_\mathsf{H}$. Par contre la réduction à un f_3-attaquant ne saute pas aux yeux, bien qu'intuitivement elle devrait exister. Il en va de même pour les réductions à des (f-)attaquants à $m\mathsf{BC}_\mathsf{H}$ qui sont significativement meilleurs que des attaquants triviaux mais moins bons que ceux nécessaires au théorème 4.2[72] et à la proposition 4.4[75]. Nous reléguons pour l'instant ces considérations au rayon des avenues de recherche et nous y reviendrons au chapitre 6 (problème P5[124]).

Chapitre 5

Transfert inconscient

5.1 Le protocole

Le protocole que nous allons étudier a été publié dans l'article de Crépeau *Quantum oblivious transfer* [Cré94], voir aussi [BBCS91]. Il ne s'agit pas à proprement parler d'un transfert inconscient *quantique*, mais plutôt de réaliser la tâche classique du transfert inconscient par l'utilisation de messages quantiques. Rappelons la nature de cette tâche cryptographique: Bob possède deux bits secrets, a_0 et a_1. Alice désire obtenir le bit a_c à condition que la valeur de c demeure secrète. De son côté, Bob est prêt à accéder au voeu d'Alice pourvu qu'Alice n'obtienne aucune information sur l'autre bit, $a_{\bar{c}}$.

En suivant le protocole de la figure 5.1[80] pas à pas, nous introduirons la terminologie qui s'y rapporte: le *bit de choix*, les *qubits BB84*, les *mises en gage*, le *test*, l'*annonce*, les *positions correctes et incorrectes.*

L'entier n sert de paramètre de sécurité. Bob se choisit aléatoirement une chaîne $\boldsymbol{b}$ de n bits et une chaîne $\boldsymbol{\theta}$ de n bases. Ces bases sont canoniques ou diagonales. Il

$$
\begin{array}{rcl}
\text{Alice}(c) & & \text{Bob}(a_0,a_1) \\
\hline
& & \boldsymbol{b} \overset{\mathcal{U}}{\leftarrow} \{0,1\}^n \\
& & \boldsymbol{\theta} \overset{\mathcal{U}}{\leftarrow} \{+,\times\}^n \\
& & |\pi\rangle \leftarrow \bigotimes_{j=1}^{n} |\boldsymbol{b}[j]\rangle_{\boldsymbol{\theta}[j]} \\
& \xleftarrow{\quad |\pi\rangle \quad} & \\
\hat{\boldsymbol{\theta}} \overset{\mathcal{U}}{\leftarrow} \{+,\times\}^n & & \\
\hat{\boldsymbol{b}} \overset{\mathbb{M}_{\hat{\boldsymbol{\theta}}}}{\leftarrow} |\pi\rangle & & \\
& \xrightarrow{\quad \boxed{\hat{\boldsymbol{\theta}}, \hat{\boldsymbol{b}}} \quad} & \\
& \xleftarrow{\quad \boldsymbol{\theta} \quad} & \\
\text{Choisir } I_0 \text{ et } I_1 \text{ tels que:} & & \\
I_0,\, I_1 \subseteq \{1,2,\ldots,n\} & & \\
I_0 \cap I_1 = \emptyset & & \\
|I_0| = |I_1| = n/3 & & \\
\forall j \in I_0 \;:\; \hat{\boldsymbol{\theta}}[j] = \boldsymbol{\theta}[j] & & \\
(J_0,J_1) \leftarrow (I_c,I_{\bar{c}}) & & \\
& \xrightarrow{\quad (J_0,J_1) \quad} & \\
& & a'_0 \leftarrow a_0 \oplus \bigoplus_{j\in J_0} \boldsymbol{b}[j] \\
& & a'_1 \leftarrow a_1 \oplus \bigoplus_{j\in J_1} \boldsymbol{b}[j] \\
& \xleftarrow{\quad (a'_0,a'_1) \quad} & \\
a_c = a'_c \oplus \bigoplus_{j\in I_0} \hat{\boldsymbol{b}}[j] & &
\end{array}
$$

Fig. 5.1 – $\mathsf{OT_S} \leq \mathsf{BC_H}$

prépare et transmet à Alice l'état quantique $|\pi\rangle$ de n qubits qui encode les bits de $\boldsymbol{b}$ dans les bases correspondantes de $\boldsymbol{\theta}$. Alice choisit à son tour aléatoirement une chaîne $\hat{\boldsymbol{\theta}}$ de n bases qu'elle utilise pour mesurer les qubits reçus de Bob. Jusqu'à maintenant, ce protocole est en tous points semblable au protocole d'échange de clef quantique que nous avons mentionné à la section 1.1[1] [BB84]. Pour cette raison, nous appelons les qubits $|\boldsymbol{b}[j]\rangle_{\boldsymbol{\theta}[j]} \in \{\ |0\rangle_{+},\ |1\rangle_{+},\ |0\rangle_{\times},\ |1\rangle_{\times}\ \}$ envoyés par Bob des *qubits BB84*.

La prochaine étape consiste, pour Bob, à annoncer ses bases $\boldsymbol{\theta}$ à Alice, et nous appelons cette étape l'*annonce*. Mais avant de procéder à cette annonce, Bob veut obtenir la garantie qu'Alice a bel et bien mesuré les qubits $|\pi\rangle$ — si Alice n'est pas tenue de mesurer $|\pi\rangle$ avant l'annonce des bases, alors on se convaincra facilement que ce protocole présente une faille béante grâce à laquelle Alice pourrait obtenir la valeur des *deux* bits, a_0 et a_1, de Bob. Cette garantie est offerte par Alice au moyen de mises en gage inconditionnellement camouflantes, d'où la réduction à $\mathsf{BC_H}$. Dans la figure 5.1[80], ces mises en gages sont indiquées au moyen d'une petite boîte qui voyage d'Alice vers Bob. Alice met donc en gage $2n$ bits, c'est-à-dire ses choix de bases $\hat{\boldsymbol{\theta}}$ et ses résultats de mesures $\hat{\boldsymbol{b}}$.

Après avoir pris connaissance des bases $\boldsymbol{\theta}$ dans lesquelles étaient encodés les bits $\boldsymbol{b}$, Alice sait à quelles positions $j \in \{1, \ldots, n\}$ elle a, par pure chance, choisit la même base que Bob, c'est-à-dire les positions j pour lesquelles $\hat{\boldsymbol{\theta}}[j] = \boldsymbol{\theta}[j]$ et $\hat{\boldsymbol{b}}[j] = \boldsymbol{b}[j]$. Alice se construit alors un ensemble $I_0 \subseteq \{1, \ldots, n\}$ de taille $n/3$ de *positions correctes* qui lui servira de masque lui permettant d'obtenir la valeur du bit a_c — c est le *bit de choix* d'Alice — comme le montre la suite du protocole à la figure 5.1[80]. La probabilité qu'Alice ne puisse constituer un tel ensemble est exponentiellement faible en n, voir la proposition 2.5[21]. Dans ces très rares cas, il est convenable pour Alice de déclarer que le protocole a échoué, de consentir à ouvrir toutes les mises en gage et que le protocole redémarre du début.

Une étape importante du protocole, qui n'est pas indiquée à la figure 5.1[80] afin d'en simplifier la présentation, consiste pour Bob à exiger l'ouverture de certaines des mises en gage d'Alice, étape que nous appelons le *test*. Cette étape a lieu entre la réception des mises en gage et l'annonce des bases $\boldsymbol{\theta}$. La moitié des positions, choisies aléatoirement par Bob, sont sacrifiées et ne jouerons plus aucun rôle dans la suite du protocole. On comprendra qu'il y a abus d'utilisation du paramètre n à la figure 5.1[80]: le *vrai* protocole consiste à envoyer $2n$ qubits, qu'Alice les mesure, qu'elle mette en gage $2n$ bits et $2n$ bases, que Bob demande l'ouverture des mises en gage de n bits et des n bases correspondantes, et que Bob annonce les n bases aux positions restantes s'il considère qu'Alice passe le test. Le test permet à Bob de s'assurer de l'honnêteté d'Alice. Si à une position j choisie pour le test Bob constate que

$$\hat{\boldsymbol{\theta}}[j] = \boldsymbol{\theta}[j]$$

mais que

$$\hat{\boldsymbol{b}}[j] \neq \boldsymbol{b}[j],$$

alors il sait qu'Alice a triché. En effet, un tel résultat est incompatible avec la prescription du protocole selon laquelle Alice doit mettre en gage son choix de base et le résultat de la mesure de $|\boldsymbol{b}[j]\rangle_{\boldsymbol{\theta}[j]}$ dans cette base. Si au moins une des positions ouvertes lors du test présente une telle anomalie, alors Bob déclare Alice malhonnête et cesse de participer. Dit autrement, Alice passe le test avec succès si, et seulement si

$$\boldsymbol{b} \oplus \hat{\boldsymbol{b}} \preceq \boldsymbol{\theta} \oplus \hat{\boldsymbol{\theta}}, \tag{5.1}$$

voir la notation 2.2[19].

Si Alice passe le test avec succès alors le protocole se déroule comme prévu à la figure 5.1[80]. Nous en continuons l'analyse à la section suivante.

5.2 La sécurité contre Bob malhonnête

C'est de ce côté-ci que les choses sont simples. La réduction se fait depuis OT_S, c'est-à-dire que le transfert devrait camoufler inconditionnellement le bit de choix c. Notre analyse sera informelle mais convaincante.

La seule information transmise à Bob qui soit corrélée avec c est la paire d'ensembles de positions (J_0, J_1). Comme le montre la figure 5.1[80], les bits de l'ensemble J_0 servent à masquer a_0, et ceux de J_1 masquent a_1. L'un de ces deux ensembles ne contient que des positions correctes et l'autre contient très probablement au moins une *position incorrecte* — la probabilité qu'Alice puisse constituer *deux* ensembles disjoints de positions correctes de tailles $n/3$ est aussi exponentiellement faible en n par la loi des grands nombres, proposition 2.5[21]. Afin de connaître la valeur du bit de choix d'Alice, Bob doit déterminer lequel de J_0 ou J_1 est un ensemble de positions où les choix de bases d'Alice coïncident avec ses choix à lui. Mais ces choix ont été faits, de part et d'autre, de façon indépendante des choix du vis-à-vis. De plus, la seule information au sujet de $\hat{\boldsymbol{\theta}}$ que Bob a reçue a été transmise au moyen de mises en gage inconditionnellement camouflantes. Nous concluons que la valeur du bit c demeure inconditionnellement inconnue de Bob à la fin du protocole.

5.3 La sécurité contre Alice malhonnête

On considère qu'Alice réussit une attaque contre le transfert inconscient si elle obtient de l'information significative sur plus d'un des deux bits a_0 et a_1. D'aucuns considèrent que si une attaquante apprend quelque chose à propos de $a_0 \oplus a_1$, le *ou exclusif* des bits secrets, alors elle aura également réussi une attaque, même si elle ignore totalement les valeurs de a_0 et a_1 [Cré01]. Par la structure du protocole de la figure 5.1[80], on se convaincra facilement que si une information sur $a_0 \oplus a_1$, ou sur tout autre valeur dépendant des deux bits, peut filtrer jusqu'à Alice, alors celle-ci obtiendra nécessairement de l'information corrélée à a_0 et à a_1.

La seule information transmise à Alice qui soit corrélée avec les deux bits secrets est cryptée dans a'_0 et a'_1. Pour décrypter a'_0 ou a'_1, Alice doit connaître ou deviner la valeur du bit de parité de deux sous-chaînes de $\boldsymbol{b}$ de son choix, dont les longueurs sont $n/3$. Rappelons que dans le cas honnête Alice apprendra à peu près la moitié des bits de la chaîne $\boldsymbol{b}$ lors de l'annonce.

Pour ce faire, Alice fait face à une alternative. D'une part, elle pourrait décider de ne pas mesurer la chaîne de qubits $|\pi\rangle$, de mettre en gage des valeurs quelconques, d'attendre l'annonce et mesurer $|\pi\rangle$ dans les bases annoncées et ainsi obtenir toute l'information sur $\boldsymbol{b}$. Une telle tactique est risquée pour Alice car elle échouera le test d'ouverture avec probabilité très proche de 1. D'autre part, elle pourrait s'engager honnêtement à toutes ses mesures afin de passer le test, et tenter d'extraire les bits de parité qu'elle désire à partir de l'information qu'elle a conservée sur les mises en gage qui n'ont pas été ouvertes. Cette possibilité n'est pas exclue a priori puisque les mises en gage ne sont que calculatoirement liantes. En fait, un éventail de stratégies s'offrent à Alice situées entre ces deux pôles: la mise en gage sur des valeurs quelconques et la mise en gage honnête. Dans tous les cas, elle essaie d'extraire des bits de parité afin d'obtenir de l'information sur les bits a_0 et a_1.

Nous ne définissons pas de façon formelle le modèle d'adversaire au côté calculatoire de $\mathsf{OT_S}$. Nous allons plutôt analyser, dans les sections 5.3.1[85] et 5.3.2[96], les propriétés cryptographiques d'un modèle calculatoire *mise en gage–extraction de bit de parité*. Nous ferons abstraction du contexte offert par le protocole de transfert inconscient et analyserons d'abord ce modèle pour lui-même. Nous reviendrons sur le lien entre ce modèle et notre protocole à la section 5.3.3[117].

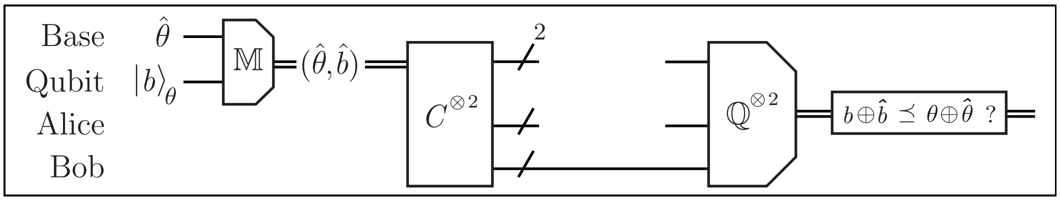


FIG. 5.2 – *Mise en gage de mesure sur un qubit*

5.3.1 Mise en gage de mesure sur un qubit

Nous démarrons notre analyse en étudiant un cas simple. Bob choisit uniformément au hasard un qubit BB84 $|b\rangle_\theta$. Alice le mesure et met en gage, de façon inconditionnellement camouflante, son choix de base, $\hat{\theta} \in \{+,\times\}$, de même que le résultat de sa mesure, $\hat{b} \in \{0,1\}$. Après la réception de ces mises en gage, Bob annonce à Alice la base θ. Après l'annonce, Alice et Bob procèdent à l'ouverture des deux mises en gage, ce qui permet à Bob de tester, comme à la ligne (5.1[82]), la bonne foi d'Alice. Ce scénario introduit la primitive de *mise en gage de mesure* et il est illustré à la figure 5.2[85] où les portes C et $\mathbb{Q}$ sont telles que définies à la figure 3.3[51]. On pourra donner un sens cryptographique à cette nouvelle primitive, dont le sigle sera QMC pour *quantum measure commitment*, lorsqu'on en aura défini l'adversaire, ce que nous nous empressons de faire.

La question qui nous intéresse est la suivante: Étant donnée une certaine probabilité de succès lors du test, et étant donnée une probabilité de succès à deviner le bit b entre l'annonce et l'ouverture, quel peut être la qualité d'un adversaire à la condition liante d'une mise en gage tel qu'entendue à la définition 3.5[53]? L'expression *entre l'annonce et l'ouverture* signifie qu'on a accès à l'annonce, mais pas au registre transmis à Bob en guise de mise en gage. Nous cherchons donc une réduction d'un adversaire $\mathcal{A}_{\mathsf{BC_H}}$ à une notion d'adversaire $\mathcal{A}_{\mathsf{QMC}}$ qui tient compte des deux probabilités de succès que nous venons de mentionner. Nous sommes prêts à énoncer la définition qui suit:

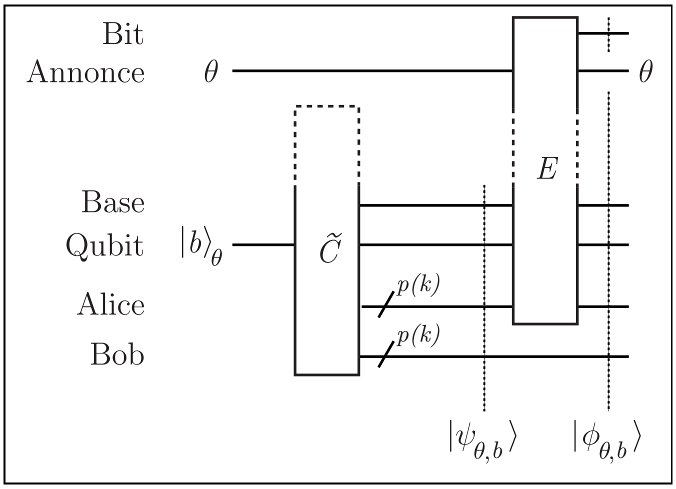


Fig. 5.3 – *Adversaire à une mise en gage de mesure sur un qubit*

Définition 5.1 (*mise en gage de mesure: adversaire*). Un *adversaire à une mise en gage de mesure* telle que modélisée à la figure 5.2[85] est une paire de familles de circuits quantiques

$$\widetilde{C} = \{\widetilde{C}_k\}_{k>0},\ \ E = \{E_k\}_{k>0}$$

qui répondent aux spécifications de la figure 5.3[86]. La porte $\widetilde{C}$ est appelée la *mise en gage malhonnête* et E est appelé l'*extracteur*. Un tel adversaire est

$$(t(k),\delta(k),\epsilon(k))\text{-bon}$$

si

$$\|\widetilde{C}\|_{\mathcal{U}} + \|E\|_{\mathcal{U}} \in O(t(k)), \tag{5.2}$$

$$\frac{1}{4}\sum_{\theta\in\{+,\times\},b\in\{0,1\}} \|(\mathbb{Q}_\theta \otimes \mathbb{Q}_b + \mathbb{Q}_{\overline{\theta}} \otimes \mathbb{Q}_b + \mathbb{Q}_{\overline{\theta}} \otimes \mathbb{Q}_{\overline{b}})|\psi_{\theta,b}\rangle\|^2 \geq \delta(k), \tag{5.3}$$

$$\frac{1}{4}\sum_{\theta,b} \|(|b\rangle^{\mathrm{Bit}}\langle b| \otimes \mathbb{1}^{\mathrm{Etc}})|\phi_{\theta,b}\rangle\|^2 \ - \ \frac{1}{2} \ \geq \epsilon(k). \tag{5.4}$$

L'entier k sert de paramètre de sécurité. Si

$$\frac{1}{4}\sum_{\theta,b} \|(\mathbb{Q}_\theta \otimes \mathbb{Q}_b + \mathbb{Q}_{\overline{\theta}} \otimes \mathbb{Q}_b + \mathbb{Q}_{\overline{\theta}} \otimes \mathbb{Q}_{\overline{b}})|\psi_{\theta,b}\rangle\|^2 = 1,$$

alors on dira que l'adversaire a une *ouverture parfaite*. Si

$$\frac{1}{4}\sum_{\theta,b} \|(|b\rangle^{\text{Bit}}\langle b| \otimes \mathbb{1}^{\text{Etc}})|\phi_{\theta,b}\rangle\|^2 = 1,$$

alors on dira que l'adversaire a un *extracteur parfait*. ▲

Quelques remarques sur la définition 5.1[86] sont nécessaires. Tout d'abord, on notera les ressemblances entre cette définition et celle d'un adversaire à la condition liante de $\mathsf{BC_H}$, définition 3.5[53]. Ensuite, trois paramètres définissent la qualité d'un adversaire à une mise en gage de mesure. Le temps requis pour réaliser l'attaque est dans l'ordre de $t(k)$, ligne (5.2[86]). La probabilité de succès lors du test est bornée inférieurement par $\delta(k)$, ligne (5.3[86]). On prend la moyenne par rapport aux choix aléatoires de θ et b, choix réalisés honnêtement par Bob. Cette inégalité aurait pu être écrite plus succinctement comme suit:

$$\frac{1}{4}\sum_{b\oplus\hat{b}\preceq\theta\oplus\hat{\theta}} \|\mathbb{Q}_{\hat{\theta},\hat{b}}|\psi_{\theta,b}\rangle\|^2 \geq \delta(k),$$

où

$$\mathbb{Q}_{\hat{\theta},\hat{b}} \equiv \mathbb{Q}_{\hat{\theta}} \otimes \mathbb{Q}_{\hat{b}}.$$

Enfin la probabilité de succès de l'extracteur E à prédire le bit b entre l'annonce et l'ouverture est bornée inférieurement par $\epsilon(k) + \frac{1}{2}$, ligne (5.4[86]). La quantité $\epsilon(k)$ est donc une borne sur le *biais* en faveur de b obtenu par E. Puisque l'annonce de la base θ est classique, on ne perd aucune généralité à présumer que l'extracteur reproduit θ en sortie, ce qui est indiqué à la figure 5.3[86].

Comme à la remarque 3.6[53], nous relevons le cas d'un adversaire *trivial*, c'est-à-dire qui ne nécessite aucune ressource qui ne soit accessible à un participant honnête.

Remarque 5.2 (*deux adversaires $\mathcal{A}_{\mathsf{QMC}}$ triviaux*). Alice peut trivialement réaliser un adversaire $(\|C\|_{\mathcal{U}}, 1, \frac{1}{4})$-bon en s'engageant honnêtement à sa mesure, comme à la figure 5.2[85], et en choisissant invariablement le bit $\mathsf{0}$ comme "extraction" de b

lorsque la base annoncée ne correspond pas à son choix. D'autre part, un adversaire trivial $(\|C\|_{\mathcal{U}}, \frac{3}{4}, \frac{1}{2})$-bon est réalisé en s'engageant invariablement à la paire $(+,\mathsf{0})$, et en mesurant le registre $\mathcal{H}^{\text{Qubit}}$ dans la base annoncée θ afin d'obtenir la valeur de b avec certitude. ▲

Il existe un spectre d'adversaires triviaux situés entre les deux pôles de la remarque 5.2[87]. D'un point de vue cryptographique, tout adversaire $\mathcal{A}_{\mathsf{QMC}}$ significativement meilleur qu'un adversaire trivial devrait permettre une réduction depuis un adversaire significativement non trivial $\mathcal{A}_{\mathsf{BC_H}}$. Nous ne ferons pas cette analyse car la présente section n'a que l'ambition pédagogique de servir de tremplin vers la mise en gage de mesure sur n qubits que nous étudirons à la section 5.3.2[96], mais nous présentons la réduction dans le cas parfait.

La réduction énoncée au théorème 5.6[94] est *non uniforme*, de même que d'autres réductions présentées aux prochaines sections, à cause de l'utilisation d'un argument combinatoire. Comme nous l'avons fait à la section 4.1[71], nous renvoyons le lecteur au chapitre 6 où on évoque la possibilité de rendre ces réductions uniformes.

La preuve du théorème 5.6[94] fait appel à trois lemmes: une réduction uniforme, un lemme combinatoire et son corollaire que voici en cascade.

Lemme 5.3 (*circuit de l'attaque*). Soient $\widetilde{C}$ et E deux familles de circuits tels que décrits à la définition 5.1[86] et à la figure 5.3[86]. Nous supposons que l'extracteur est parfait, c'est-à-dire:

$$\forall\, \theta \in \{+,\times\}, b \in \{\mathsf{0},\mathsf{1}\} \;:\; |\phi_{\theta,b}\rangle \equiv |b\rangle|\varphi_{\theta,b}\rangle. \tag{5.5}$$

Alors les quatre états $|\psi_{+,\mathsf{0}}\rangle$, $|\psi_{+,\mathsf{1}}\rangle$, $|\psi_{\times,\mathsf{0}}\rangle$ et $|\psi_{\times,\mathsf{1}}\rangle$ peuvent être préparés *localement* au moyen des portes $\widetilde{C}$ et E. Plus précisément, nous montrons qu'il est possible de produire les quatre $|\psi_{\theta,b}\rangle$ sans toucher au registre $\mathcal{H}^{\text{Bob}}$ après qu'un unique message quantique de mise en gage soit transmis à Bob.

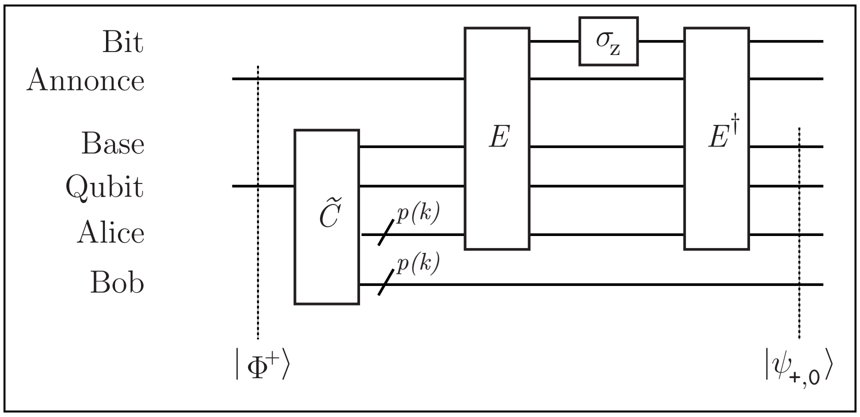


FIG. 5.4 – *Préparation locale de $|\psi_{+,0}\rangle$ étant donné $\mathcal{A}_{\mathsf{QMC}}$ parfait*

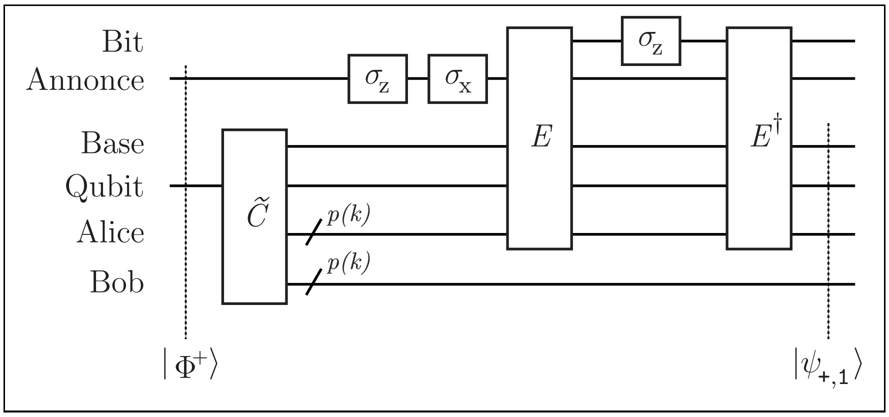


FIG. 5.5 – *Préparation locale de $|\psi_{+,1}\rangle$ étant donné $\mathcal{A}_{\mathsf{QMC}}$ parfait*

Preuve. La réduction apparaît aux figures 5.4[89] à 5.7[90], où $|\Phi^+\rangle$ désigne l'état de Bell:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|\mathsf{00}\rangle + |\mathsf{11}\rangle).$$

Vérifions étape par étape la validité du circuit de la figure 5.4[89]:

$$\begin{aligned}
&|\vdash\rangle^{\mathrm{Etc}}|\Phi^+\rangle^{\mathrm{Annonce,Qubit}} \\
&\quad = \quad \frac{1}{\sqrt{2}}|\vdash\rangle|\mathsf{0}\rangle|\mathsf{0}\rangle_+ \;+\; \frac{1}{\sqrt{2}}|\vdash\rangle|\mathsf{1}\rangle|\mathsf{1}\rangle_+ \\
&\quad \overset{\tilde{C}}{\longmapsto} \quad \frac{1}{\sqrt{2}}|\mathsf{0}\rangle|\psi_{+,\mathsf{0}}\rangle \;+\; \frac{1}{\sqrt{2}}|\mathsf{1}\rangle|\psi_{+,\mathsf{1}}\rangle
\end{aligned} \tag{5.6}$$

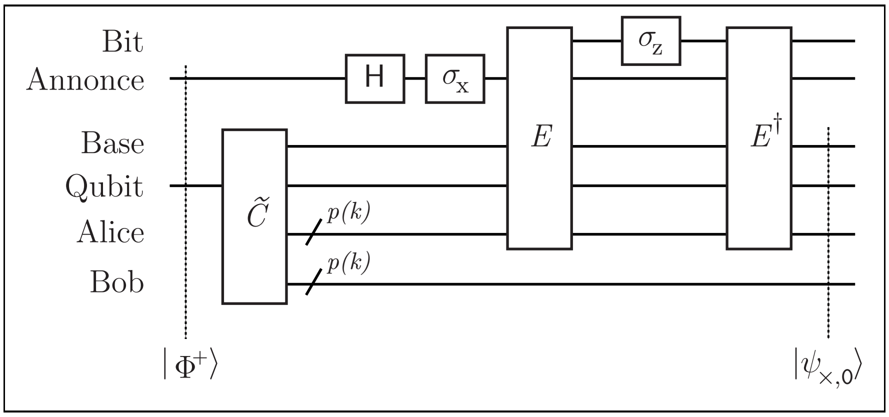


Fig. 5.6 – *Préparation locale de $|\psi_{\times,0}\rangle$ étant donné $\mathcal{A}_{\mathsf{QMC}}$ parfait*

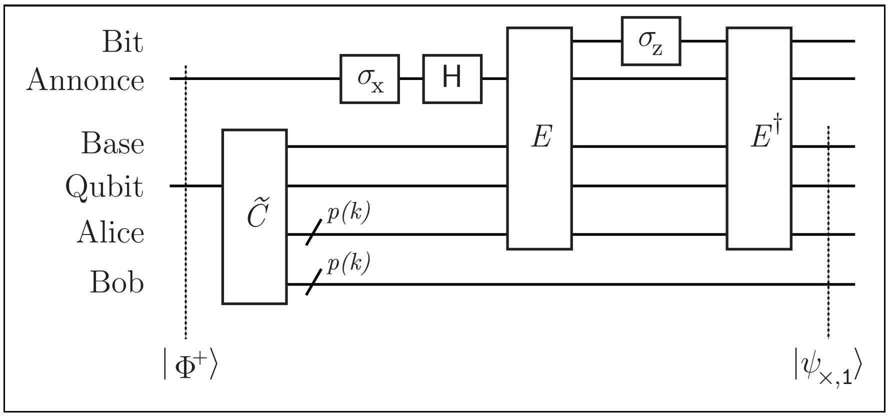


Fig. 5.7 – *Préparation locale de $|\psi_{\times,1}\rangle$ étant donné $\mathcal{A}_{\mathsf{QMC}}$ parfait*

$$
\begin{aligned}
&= \quad \frac{1}{\sqrt{2}}|0\rangle|\psi_{+,0}\rangle \ + \ \frac{1}{\sqrt{2}}|1\rangle(\frac{1}{\sqrt{2}}|\psi_{\times,0}\rangle - \frac{1}{\sqrt{2}}|\psi_{\times,1}\rangle) && (5.7)\\
&= \quad \frac{1}{\sqrt{2}}|0\rangle|\psi_{+,0}\rangle \ + \ \frac{1}{2}|1\rangle|\psi_{\times,0}\rangle - \frac{1}{2}|1\rangle|\psi_{\times,1}\rangle \\
&\overset{E^\dagger\sigma_z E}{\longmapsto} \quad \frac{1}{\sqrt{2}}|0\rangle|\psi_{+,0}\rangle \ + \ \frac{1}{2}|1\rangle|\psi_{\times,0}\rangle + \frac{1}{2}|1\rangle|\psi_{\times,1}\rangle && (5.8)\\
&= \quad \frac{1}{\sqrt{2}}|0\rangle|\psi_{+,0}\rangle \ + \ \frac{1}{\sqrt{2}}|1\rangle(\frac{1}{\sqrt{2}}|\psi_{\times,0}\rangle + \frac{1}{\sqrt{2}}|\psi_{\times,1}\rangle) \\
&= \quad \frac{1}{\sqrt{2}}|0\rangle|\psi_{+,0}\rangle \ + \ \frac{1}{\sqrt{2}}|1\rangle|\psi_{+,0}\rangle && (5.9)\\
&= \quad (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)|\psi_{+,0}\rangle.
\end{aligned}
$$

La ligne (5.6[89]) est due à la propriété suivante de la porte $\widetilde{C}$:

$$\forall\ \theta \in \{+,\times\}, b \in \{0,1\} \ : \ |\psi_{\theta,b}\rangle = \widetilde{C}(|\vdash\rangle^{\text{Etc}}|b\rangle_\theta^{\text{Qubit}}),$$

que l'on peut vérifier par inspection de la figure 5.3[86]. Les lignes (5.7[91]) et (5.9[91]) viennent des identités (2.2[26]) et (2.1[26]) respectivement auxquelles on aura appliqué la transformation linéaire $\widetilde{C}$. Enfin la ligne (5.8[91]) est obtenue à l'aide de la propriété suivante de l'extracteur E:

$$\forall\ \theta \in \{+,\times\}, b \in \{0,1\} \ : \ E^\dagger\sigma_z E(|\theta\rangle^{\text{Annonce}}|\psi_{\theta,b}\rangle) = (-1)^b|\theta\rangle|\psi_{\theta,b}\rangle,$$

qui peut elle aussi être vérifiée par inspection de la figure 5.3[86] et en remarquant que le changement de phase est fait conditionnellement à la valeur du bit extrait par E. C'est là que la perfection de l'extracteur est utilisée, voir la ligne (5.5[88]).

Trois autres calculs, semblables à celui que nous venons de faire et que nous omettons, permettent de vérifier la validité des circuits présentés aux figures 5.5[89], 5.6[90] et 5.7[90]. ■

Lemme 5.4 (*lemme combinatoire*). Considérons un tableau $\boldsymbol{T}$ de 4 lignes par 3 colonnes. Les lignes sont indexées par les 4 paires $(\theta,b) \in \{0,1\}^2$ et les colonnes sont indexées par les 3 paires $(\tau,c) \in \{\mathtt{0},\mathtt{1}\}^2$ telles que $c \preceq \tau$. On considère également 12 sous-tableaux, tous de dimensions 2×2, constitués des cases qui sont à l'intersection de certaines lignes et certaines colonnes de $\boldsymbol{T}$. Les 12 sous-tableaux sont en bijection avec les 12 choix possibles de valeurs des 3 paramètres suivants:

$$r \in \{1,2,3\},\ u \in \{\mathtt{0},\mathtt{1}\},\ v \in \{\mathtt{0},\mathtt{1}\}.$$

Soient $r \in \{1,2,3\}$ et $u,v \in \{\mathtt{0},\mathtt{1}\}$ fixés. La ligne (θ,b) fait partie du sous-tableau (r,u,v) selon les conditions suivantes:

$$r = 1 \implies (\theta,b) \in \{(\mathtt{1},u),(\mathtt{0},v)\}, \tag{5.10}$$

$$r = 2 \implies (\theta,b) \in \{(u,\mathtt{0}),(v,\mathtt{1})\}, \tag{5.11}$$

$$r = 3 \implies (\theta,b) \in \{(u,u),(v,\overline{v})\}. \tag{5.12}$$

La colonne (τ,c) fait partie du sous-tableau (r,u,v) selon les conditions suivantes:

$$r = 1 \implies (\tau,c) \in \{(\mathtt{1},\mathtt{0}),(\mathtt{1},\mathtt{1})\}, \tag{5.13}$$

$$r = 2 \implies (\tau,c) \in \{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{0})\}, \tag{5.14}$$

$$r = 3 \implies (\tau,c) \in \{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{1})\}. \tag{5.15}$$

Alors toute case de $\boldsymbol{T}$ appartient à exactement 4 sous-tableaux.

Preuve. Soit (θ,b,τ,c), avec $c \preceq \tau$, une case de $\boldsymbol{T}$. Par inspection des conditions (5.10[92]) à (5.15[92]), on établit exhaustivement la liste des sous-tableaux auxquels appartient cette case, voir la figure 5.8[93]. ■

Lemme 5.5 (*corollaire du lemme 5.4*[91]). Supposons que chaque case du tableau $\boldsymbol{T}$ contient un nombre réel positif, et soit T le grand total des cases de $\boldsymbol{T}$. Alors il existe un sous-tableau dont la somme des cases est au moins $T/3$.

Preuve. La somme de tous les sous-tableaux doit être de $4T$ puisque chaque case appartient à exactement 4 sous-tableaux. Comme on considère exactement 12 sous-tableaux, alors ils ne peuvent pas tous être inférieurs à $4T/12 = T/3$. ■

0000	0010	0011	0100	0110	0111	1000	1010	1011	1100	1110	1111
	(1,0,0)	(1,0,0)					(1,0,0)	(1,0,0)			
				(1,0,1)	(1,0,1)		(1,0,1)	(1,0,1)			
	(1,1,0)	(1,1,0)								(1,1,0)	(1,1,0)
				(1,1,1)	(1,1,1)					(1,1,1)	(1,1,1)
(2,0,0)	(2,0,0)		(2,0,0)	(2,0,0)							
(2,0,1)	(2,0,1)								(2,0,1)	(2,0,1)	
			(2,1,0)	(2,1,0)		(2,1,0)	(2,1,0)				
						(2,1,1)	(2,1,1)		(2,1,1)	(2,1,1)	
(3,0,0)		(3,0,0)	(3,0,0)		(3,0,0)						
(3,0,1)		(3,0,1)				(3,0,1)		(3,0,1)			
			(3,1,0)		(3,1,0)				(3,1,0)		(3,1,0)
						(3,1,1)		(3,1,1)	(3,1,1)		(3,1,1)

Fig. 5.8 – *Lemme combinatoire: triplets (r,u,v) admissibles pour chaque $(\theta,b,_{\top},c)$*

Théorème 5.6 ($\mathcal{A}^1_{\mathsf{2BC_H}} \leq_\exists \mathcal{A}_{\mathsf{QMC}}$, *cas parfait*). Soient $\widetilde{C}$ et E deux familles de circuits tels que décrits à la définition 5.1[86] et à la figure 5.3[86], attaquant le QMC de la figure 5.2[85]. Nous supposons que cette attaque a une ouverture parfaite et un extracteur parfait, c'est-à-dire:

$$\forall\, \theta \in \{+,\times\}, b \in \{\mathsf{0},\mathsf{1}\} \;:\; \|(\mathbb{Q}_{\theta,b} + \mathbb{Q}_{\overline{\theta},b} + \mathbb{Q}_{\overline{\theta},\overline{b}})|\psi_{\theta,b}\rangle\|^2 = 1 \tag{5.16}$$

et

$$\forall\, \theta \in \{+,\times\}, b \in \{\mathsf{0},\mathsf{1}\} \;:\; |\phi_{\theta,b}\rangle \equiv |b\rangle|\varphi_{\theta,b}\rangle.$$

Alors il existe une f-attaque à $\mathsf{2BC_H}$ $(\|\widetilde{C}\|_{\mathcal{U}} + \|E\|_{\mathcal{U}},\, \frac{1}{3})$-bonne, voir la définition 4.6[76], où f elle l'une des 3 fonctions suivantes:

$$\begin{aligned}
f_1 &: \{\mathsf{0},\mathsf{1}\}^2 \longrightarrow \{\mathsf{0},\mathsf{1}\} \;:\; (\theta,b) \longmapsto \theta,\\
f_2 &: \{\mathsf{0},\mathsf{1}\}^2 \longrightarrow \{\mathsf{0},\mathsf{1}\} \;:\; (\theta,b) \longmapsto b,\\
f_3 &: \{\mathsf{0},\mathsf{1}\}^2 \longrightarrow \{\mathsf{0},\mathsf{1}\} \;:\; (\theta,b) \longmapsto \theta \oplus b.
\end{aligned}$$

Preuve. La clef de la f-attaque à $\mathsf{2BC_H}$ cherchée réside dans les quatre états $|\psi_{\theta,b}\rangle$, pour $\theta \in \{+,\times\}$ et $b \in \{\mathsf{0},\mathsf{1}\}$. Le lemme 5.3[88] montre qu'il est possible de produire localement chacun des états $|\psi_{\theta,b}\rangle$ comme l'exige la définition 4.6[76] et le montre la figure 3.4[53].

La preuve du théorème se poursuit par un argument combinatoire qui établit l'existence de deux états, parmi les quatre $|\psi_{\theta,b}\rangle$, qui incarnent une f-attaque à $\mathsf{2BC_H}$.

La ligne (5.16[94]) peut être récrite comme suit:

$$\|\mathbb{Q}_{+,\mathsf{0}}|\psi_{+,\mathsf{0}}\rangle\|^2 + \|\mathbb{Q}_{\times,\mathsf{0}}|\psi_{+,\mathsf{0}}\rangle\|^2 + \|\mathbb{Q}_{\times,\mathsf{1}}|\psi_{+,\mathsf{0}}\rangle\|^2 = 1, \tag{5.17}$$

$$\|\mathbb{Q}_{+,\mathsf{1}}|\psi_{+,\mathsf{1}}\rangle\|^2 + \|\mathbb{Q}_{\times,\mathsf{1}}|\psi_{+,\mathsf{1}}\rangle\|^2 + \|\mathbb{Q}_{\times,\mathsf{0}}|\psi_{+,\mathsf{1}}\rangle\|^2 = 1, \tag{5.18}$$

$$\|\mathbb{Q}_{\times,\mathsf{0}}|\psi_{\times,\mathsf{0}}\rangle\|^2 + \|\mathbb{Q}_{+,\mathsf{0}}|\psi_{\times,\mathsf{0}}\rangle\|^2 + \|\mathbb{Q}_{+,\mathsf{1}}|\psi_{\times,\mathsf{0}}\rangle\|^2 = 1, \tag{5.19}$$

$$\|\mathbb{Q}_{\times,\mathsf{1}}|\psi_{\times,\mathsf{1}}\rangle\|^2 + \|\mathbb{Q}_{+,\mathsf{1}}|\psi_{\times,\mathsf{1}}\rangle\|^2 + \|\mathbb{Q}_{+,\mathsf{0}}|\psi_{\times,\mathsf{1}}\rangle\|^2 = 1, \tag{5.20}$$

en invoquant l'orthogonalité des projecteurs $\mathbb{Q}_{+,0}$, $\mathbb{Q}_{+,1}$, $\mathbb{Q}_{\times,0}$ et $\mathbb{Q}_{\times,1}$, voir la proposition 2.22[32].

Les lignes (5.17[94]) à (5.20[94]) forment un tableau de dimensions 4×3 que nous baptisons $\boldsymbol{T}$. La case (θ,b,τ,c) de $\boldsymbol{T}$ contient la quantité $\|\mathbb{Q}_{\theta\oplus\tau,b\oplus c}|\psi_{\theta,b}\rangle\|^2$, de telle sorte que les lignes de $\boldsymbol{T}$ sont indexées par (θ,b) et les colonnes sont indexées par (τ,c) comme dans le lemme 5.4[91]. Le grand total de $\boldsymbol{T}$ est 4. Par le lemme 5.5[92], $\boldsymbol{T}$ doit admettre un sous-tableau de dimensions 2×2 dont la somme des cases est au moins 4/3. Suivant les mêmes paramètres des sous-tableaux présentés dans l'énoncé du lemme 5.4[91], soit (r,u,v) le sous-tableau de $\boldsymbol{T}$ dont la somme est au moins 4/3. L'examen du tableau $\boldsymbol{T}$ aux lignes (5.17[94]) à (5.20[94]) et des lignes (5.10[92]) à (5.15[92]) montre que les 4 cases du sous-tableau (r,u,v) correspondent

aux 4 termes de la ligne (4.8[78]) si $r = 1$,

ou aux 4 termes de la ligne (4.9[78]) si $r = 2$,

ou aux 4 termes de la ligne (4.10[78]) si $r = 3$,

où les deux états $|\zeta_0\rangle$ et $|\zeta_1\rangle$ sont représentés par

$|\psi_{\times,u}\rangle$ et $|\psi_{+,v}\rangle$ si $r = 1$,

ou $|\psi_{u,0}\rangle$ et $|\psi_{v,1}\rangle$ si $r = 2$,

ou $|\psi_{u,u}\rangle$ et $|\psi_{v,\overline{v}}\rangle$ si $r = 3$.

Ces deux états incarnent une f_r-attaque sur les deux bits de la mise en gage de mesure de la figure 5.2[85]. Cette f_r-attaque sera $(\|\widetilde{C}\|_{\mathcal{U}} + \|E\|_{\mathcal{U}}, \frac{1}{3})$-bonne au sens de la définition 4.6[76] et comme le montrent les figures 5.4[89] à 5.7[90]. ■

Un autre argument combinatoire, plus simple que celui du lemme 5.4[91], nous donne cette fois un adversaire $\mathcal{A}_{\mathsf{2BC_H}}$ ordinaire, c'est-à-dire au sens de la définition 4.1[71].

Théorème 5.7 ($\mathcal{A}_{\mathsf{2BC_H}} \leq_\exists \mathcal{A}_{\mathsf{QMC}}$, *cas parfait*). Soient $\widetilde{C}$ et E deux familles de circuits tels que décrits à la définition 5.1[86] et à la figure 5.3[86], attaquant le QMC de la figure 5.2[85]. Comme pour le théorème 5.6[94], nous supposons que cette attaque a une ouverture parfaite et un extracteur parfait, voir les lignes (5.17[94]) à (5.20[94]) et (5.5[88]). Alors il existe une attaque à $2\mathsf{BC}_\mathsf{H}$ $(\|\widetilde{C}\|_{\mathcal{U}} + \|E\|_{\mathcal{U}},\ \frac{1}{3})$-bonne, voir la définition 4.1[71].

Preuve. Comme au théorème 5.6[94], on invoque le lemme 5.3[88] qui nous assure que les quatre états $|\psi_{\theta,b}\rangle$ peuvent être préparés localement après que la mise en gage malhonnête soit transmise à Bob.

L'argument combinatoire est maintenant le suivant. Les lignes (5.17[94]) à (5.20[94]) forment un tableau $\boldsymbol{T}$ de format 4×3. La somme de toutes les cases est 4, donc l'une des trois colonnes doit avoir une somme d'au moins $4/3$, d'où:

$$\|\mathbb{Q}_{+,\mathtt{0}}|\psi_{\tau,c}\rangle\|^2 + \|\mathbb{Q}_{+,\mathtt{1}}|\psi_{\tau,\bar{c}}\rangle\|^2 + \|\mathbb{Q}_{\times,\mathtt{0}}|\psi_{\bar{\tau},c}\rangle\|^2 + \|\mathbb{Q}_{\times,\mathtt{1}}|\psi_{\bar{\tau},\bar{c}}\rangle\|^2 - 1 \geq \frac{1}{3} \tag{5.21}$$

pour une certaine colonne d'index (τ,c) de $\boldsymbol{T}$ avec $c \preceq \tau$. La ligne (5.21[96]) correspond à la ligne (4.1[72]) de la définition 4.1[71]. ■

5.3.2 Mise en gage de mesure sur n qubits

Le but de la présente section est de généraliser à n qubits le travail fait à la section précédente. La lecture de la section 5.3.1[85] est donc un préalable essentiel à l'étude que nous entreprenons maintenant.

Le scénario honnête de base est maintenant le suivant: Bob choisit uniformément au hasard n qubits BB84 $|\boldsymbol{b}\rangle_{\boldsymbol{\theta}}$ qu'il transmet à Alice. Alice les mesure et met en gage, de façon inconditionnellement camouflante, ses choix de bases, $\hat{\boldsymbol{\theta}} \in \{+,\times\}^n$, de même que les résultats de ses mesures, $\hat{\boldsymbol{b}} \in \{\mathtt{0},\mathtt{1}\}^n$. Après la réception de ces $2n$ mises en gage, Bob annonce à Alice les bases $\boldsymbol{\theta}$. Après l'annonce, Alice et Bob procèdent à l'ouverture des mises en gage. Bob considère qu'Alice passe le test avec succès si, et seulement si

$$\boldsymbol{b} \oplus \hat{\boldsymbol{b}} \preceq \boldsymbol{\theta} \oplus \hat{\boldsymbol{\theta}}. \tag{5.22}$$

Ce protocole est donc équivalent à n copies de la figure 5.2[85] où le résultat du test (5.22[97]) est donné par le *et* logique des tests sur chacune des n positions, et où les portes C et $\mathbb{Q}$ sont définies à la figure 3.3[51].

L'entier n est clairement un paramètre de sécurité pour l'interaction que l'on vient de décrire, et il en va de même pour le protocole de transfert inconscient présenté à la section 5.1[79]. De plus, la sécurité de chacune des $2n$ mises en gage est paramétrée par k. Afin de simplifier et clarifier la démarche qui va suivre, on lie une fois pour toute le paramètre n au paramètre de sécurité k sous-jacent aux mises en gage utilisées:

$$n \equiv k.$$

À cet égard, les remarques 4.5[76] et 4.7[77] doivent être gardées fraîchement en mémoire. Nous notons cette primitive cryptographique par $n\mathsf{QMC}$ et voici la définition formelle de son adversaire:

Définition 5.8 (*mise en gage de mesure sur n qubits: adversaire*). Un *adversaire à une mise en gage de mesure sur n qubits* est une paire de familles de circuits quantiques

$$\widetilde{C} = \{\widetilde{C}_n\}_{n>0}, \ \ E = \{E_n\}_{n>0}$$

qui se conforment aux spécifications de la figure 5.9[99]. Le scénario honnête correspond à n copies de la figure 5.2[85]. La porte $\widetilde{C}$ est appelée la *mise en gage malhonnête* et E est appelé l'*extracteur*. Un tel adversaire est

$$(t(n),\delta(n),\epsilon(n))\text{-bon}$$

si

$$\|\widetilde{C}\|_{\mathcal{U}} + \|E\|_{\mathcal{U}} \in O(t(n));$$

si

$$\frac{1}{4^n} \sum_{\substack{\boldsymbol{\theta}\in\{+,\times\}^n \\ \boldsymbol{b}\in\{0,1\}^n}} \|(\sum_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}\,:\,\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}})|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 \geq \delta(n) \tag{5.23}$$

où

$$\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}} \equiv \bigotimes_{j=1}^{n} \mathbb{Q}_{\hat{\boldsymbol{\theta}}[j]} \otimes \mathbb{Q}_{\hat{\boldsymbol{b}}[j]};$$

et si

$$\frac{1}{4^n} \sum_{\boldsymbol{\theta},\boldsymbol{b}} \|\mathbb{P}_{\|\boldsymbol{b}\|}|\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 \;-\; \frac{1}{2} \geq \epsilon(n) \tag{5.24}$$

où

$$\mathbb{P}_{\|\boldsymbol{b}\|} \equiv |\|\boldsymbol{b}\|\rangle^{\text{Parité}}\langle\|\boldsymbol{b}\|| \otimes \mathbb{1}^{\text{Etc}}. \tag{5.25}$$

L'entier n sert de paramètre de sécurité. Si

$$\frac{1}{4^n} \sum_{\boldsymbol{\theta},\boldsymbol{b}} \|(\sum_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}\,:\,\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}})|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 = 1$$

alors on dira que l'adversaire a une *ouverture parfaite*. Si

$$\frac{1}{4^n} \sum_{\boldsymbol{\theta},\boldsymbol{b}} \|\mathbb{P}_{\|\boldsymbol{b}\|}|\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 = 1$$

alors on dira que l'adversaire a un *extracteur parfait*. ▲

Notons que la sommation de la ligne (5.23[98]), qui est une moyenne prise sur les $(\boldsymbol{\theta},\boldsymbol{b})$ des probabilités de passer le test de la ligne (5.22[97]), peut être récrite plus simplement

$$\frac{1}{4^n} \sum_{\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \|\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2$$

en invoquant l'orthogonalité des projecteurs $\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}$ et la proposition 2.22[32]. La sommation de la ligne (5.24[98]) est une moyenne prise sur les $(\boldsymbol{\theta},\boldsymbol{b})$ des probabilités d'extraire avec succès, entre la mise en gage et l'ouverture, le bit de parité $\|\boldsymbol{b}\|$.

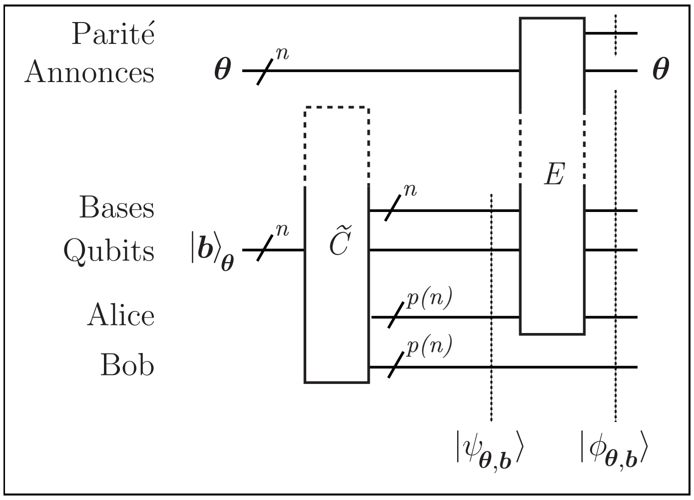


FIG. 5.9 – *Adversaire à une mise en gage de mesure sur n qubits*

Les deux pôles des adversaires triviaux sont les suivants:

Remarque 5.9 (*deux adversaires $\mathcal{A}_{n\mathsf{QMC}}$ triviaux*). On peut trivialement réaliser un adversaire $(n\|C\|_{\mathcal{U}}, 1, 0)$-bon en s'engageant honnêtement à toutes les mesures, comme à la figure 5.2[85], et en choisissant invariablement le bit $\mathsf{0}$ comme "extraction" de $\|\boldsymbol{b}\|$. D'autre part, un adversaire trivial $(n\|C\|_{\mathcal{U}}, (\frac{3}{4})^n, \frac{1}{2})$-bon est réalisé en s'engageant invariablement à la chaîne de $2n$ bits $(+,\mathsf{0})^n$, et en mesurant le registre $\mathcal{H}^{\text{Qubits}}$ dans les bases annoncées $\boldsymbol{\theta}$ afin d'obtenir la valeur de $\|\boldsymbol{b}\|$ avec certitude. ▲

5.3.2.1 Le cas parfait

Nous entreprenons maintenant la preuve du théorème 5.14[107], généralisation du théorème 5.6[94]. La structure de la preuve sera la même: les lemmes 5.3[88], 5.4[91] et 5.5[92] sont généralisés aux lemmes 5.10[99], 5.11[103] et 5.13[107] respectivement, et les circuits des figures 5.4[89] à 5.7[90] sont généralisés par l'unique circuit de la figure 5.10[100].

Lemme 5.10 (*circuit de l'attaque pour $\mathcal{A}_{n\mathsf{QMC}}$*). Soient $\widetilde{C}$ et E deux familles de

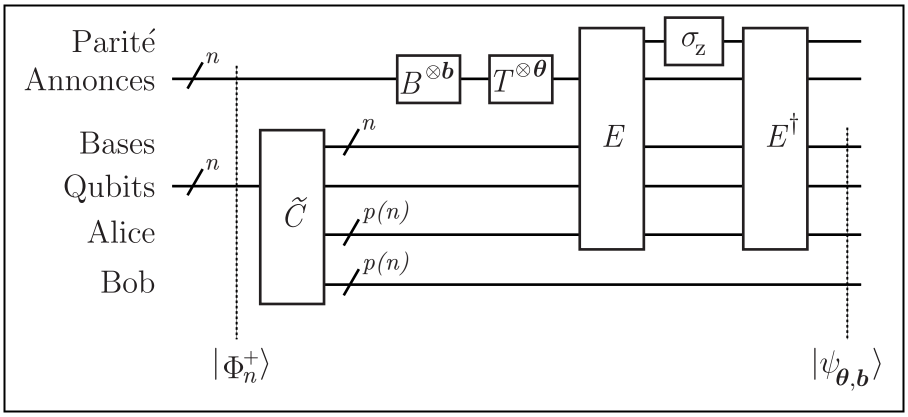


Fig. 5.10 – *Préparation locale de $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ étant donné $\mathcal{A}_{n\mathsf{QMC}}$ parfait*

circuits tels que décrits à la définition 5.8[97] et à la figure 5.9[99]. Nous supposons que l'extracteur est parfait, c'est-à-dire:

$$\forall\, \boldsymbol{\theta} \in \{+,\times\}^n,\ \boldsymbol{b} \in \{0,1\}^n\ :\ |\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \equiv |\|\boldsymbol{b}\|\rangle|\varphi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle. \tag{5.26}$$

Alors chacun des 4^n états $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$, pour $\boldsymbol{\theta} \in \{+,\times\}^n$ et $\boldsymbol{b} \in \{0,1\}^n$, peut être préparé au moyen des portes $\widetilde{C}$ et E sans toucher au registre $\mathcal{H}^{\mathrm{Bob}}$ après qu'un même message quantique de mise en gage soit transmis à Bob.

Preuve. La réduction apparaît à la figure 5.10[100] où:

$$\begin{aligned}
|\Phi_n^+\rangle &\equiv \sum_{\boldsymbol{s}\in\{0,1\}^n} \frac{1}{\sqrt{2}^n}|\boldsymbol{s}\rangle|\boldsymbol{s}\rangle,\\
B &\equiv \sigma_x\sigma_z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\\
T &\equiv \mathsf{H}\sigma_z = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.
\end{aligned}$$

Vérifions la validité du circuit de la figure 5.10[100] en omettant les justifications qui sont semblables à celles invoquées dans la preuve du lemme 5.3[88]:

$$
\begin{aligned}
&|\vdash\rangle^{\text{Etc}} |\Phi_n^+\rangle^{\text{Annonces,Qubits}} \\
&\quad = \quad |\vdash\rangle \sum_{\boldsymbol{s}} \frac{1}{\sqrt{2}^n} |\boldsymbol{s}\rangle |\boldsymbol{s}\rangle \\
&\quad \overset{\widetilde{C}}{\longmapsto} \quad \sum_{\boldsymbol{s}} \frac{1}{\sqrt{2}^n} |\boldsymbol{s}\rangle |\psi_{+^n,\boldsymbol{s}}\rangle \\
&\quad \overset{B^{\otimes \boldsymbol{b}}}{\longmapsto} \quad \sum_{\boldsymbol{s}} \frac{(-1)^{\boldsymbol{b} \odot \boldsymbol{s}}}{\sqrt{2}^n} |\boldsymbol{b} \oplus \boldsymbol{s}\rangle |\psi_{+^n,\boldsymbol{s}}\rangle && (5.27) \\
&\quad \overset{T^{\otimes \boldsymbol{\theta}}}{\longmapsto} \quad \sum_{\boldsymbol{s},\boldsymbol{t} \,:\, \boldsymbol{t} \preceq \boldsymbol{\theta}} \frac{(-1)^{\boldsymbol{b} \odot \boldsymbol{s} \,\oplus\, \boldsymbol{b} \odot \boldsymbol{t} \,\oplus\, \boldsymbol{s} \odot \boldsymbol{t}}}{\sqrt{2}^{n+|\boldsymbol{\theta}|}} |\boldsymbol{b} \oplus \boldsymbol{s} \oplus \boldsymbol{t}\rangle |\psi_{+^n,\boldsymbol{s}}\rangle. && (5.28)
\end{aligned}
$$

La ligne (5.27[101]) se justifie par la propriété de la transformation B:

$$\forall \boldsymbol{b},\boldsymbol{s} \in \{0,1\}^n \;:\; B^{\otimes \boldsymbol{b}} |\boldsymbol{s}\rangle = (-1)^{\boldsymbol{b} \odot \boldsymbol{s}} |\boldsymbol{b} \oplus \boldsymbol{s}\rangle,$$

et la ligne (5.28[101]) s'obtient de la propriété de T:

$$\forall \boldsymbol{\theta},\boldsymbol{r} \in \{0,1\}^n \;:\; T^{\otimes \boldsymbol{\theta}} |\boldsymbol{r}\rangle = \sum_{\boldsymbol{t} \,:\, \boldsymbol{t} \preceq \boldsymbol{\theta}} \frac{(-1)^{\boldsymbol{r} \odot \boldsymbol{t}}}{\sqrt{2}^{|\boldsymbol{\theta}|}} |\boldsymbol{r} \oplus \boldsymbol{t}\rangle.$$

À cette étape du circuit, nous voulons utiliser la propriété suivante de l'extracteur E:

$$\forall \boldsymbol{\theta},\boldsymbol{b} \;:\; E^\dagger \sigma_z E(|\boldsymbol{\theta}\rangle^{\text{Annonces}} |\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle) = (-1)^{\|\boldsymbol{b}\|} |\boldsymbol{\theta}\rangle |\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \tag{5.29}$$

qui s'obtient par inspection de la figure 5.9[99] et en utilisant la perfection de l'extracteur supposée à ligne (5.26[100]). De la ligne (5.28[101]), on doit d'abord récrire l'état $|\psi_{+^n,\boldsymbol{s}}\rangle$ dans la base $\boldsymbol{b} \oplus \boldsymbol{s} \oplus \boldsymbol{t}$ avant d'utiliser (5.29[101]). La formule de changement de base (2.14[41]) arrive à notre rescousse et elle peut être récrite comme suit en lui appliquant la transformation linéaire $\widetilde{C}$:

$$\forall \boldsymbol{\theta},\boldsymbol{b},\boldsymbol{w} \;:\; |\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle = \sum_{\boldsymbol{v} \,:\, \boldsymbol{v} \preceq \boldsymbol{w}} \frac{(-1)^{\boldsymbol{b} \odot \boldsymbol{w} \,\oplus\, \boldsymbol{b} \odot \boldsymbol{v}}}{\sqrt{2}^{|\boldsymbol{w}|}} |\psi_{\boldsymbol{\theta} \oplus \boldsymbol{w},\boldsymbol{b} \oplus \boldsymbol{v}}\rangle. \tag{5.30}$$

À l'aide de (5.30[101]) puis de (5.29[101]), on continue le travail laissé en (5.28[101]):

$$= \sum_{\substack{s,t,v\ :\ t\preceq\theta \\ v\preceq b\oplus s\oplus t}} \frac{(-1)^{b\odot t\ \oplus\ s\odot v\ \oplus\ s\odot s}}{\sqrt{2}^{n+|\theta|+|b\oplus s\oplus t|}} |b\oplus s\oplus t\rangle|\psi_{b\oplus s\oplus t, s\oplus v}\rangle$$

$$\overset{E^\dagger\sigma_z E}{\longmapsto} \sum_{\substack{s,t,v\ :\ t\preceq\theta \\ v\preceq b\oplus s\oplus t}} \frac{(-1)^{b\odot t\ \oplus\ s\odot v\ \oplus\ v\odot v}}{\sqrt{2}^{n+|\theta|+|b\oplus s\oplus t|}} |b\oplus s\oplus t\rangle|\psi_{b\oplus s\oplus t, s\oplus v}\rangle$$

$$\boxed{\begin{array}{l} x \equiv b\oplus s\oplus t\oplus\theta \quad \text{et} \quad y\equiv s\oplus v\oplus b \\ s = b\oplus y\oplus v \quad \text{et} \quad t=\theta\oplus x\oplus y\oplus v \end{array}}$$

$$= \sum_{\substack{x,y,v\ :\ v\oplus x\oplus y\preceq\theta \\ v\preceq\theta\oplus x}} \frac{(-1)^{b\odot\theta\ \oplus\ b\odot x\ \oplus\ b\odot y\ \oplus\ v\odot y}}{\sqrt{2}^{n+|\theta|+|\theta\oplus x|}} |\theta\oplus x\rangle|\psi_{\theta\oplus x, b\oplus y}\rangle. \quad (5.31)$$

La prochaine étape du calcul consiste à évaluer la somme

$$\sum_{\substack{v\ :\ v\oplus x\oplus y\preceq\theta \\ v\preceq\theta\oplus x}} (-1)^{v\odot y} \quad (5.32)$$

pour x, y et θ fixés. Si $y\preceq x$, alors $\forall j\in\{1,\ldots,n\}$: le bit $v[j]$ est uniquement déterminé sauf aux positions où $\theta[j]=1$ et $x[j]=0$ et dans ces cas $v[j]\wedge y[j]=0$ quel que soit la valeur de $v[j]$, d'où:

$$y\preceq x \implies \sum_{\substack{v\ :\ v\oplus x\oplus y\preceq\theta \\ v\preceq\theta\oplus x}} (-1)^{v\odot y} = 2^{|\theta\wedge\bar{x}|}. \quad (5.33)$$

Si $y\not\preceq x$, alors $\exists j^*\in\{1,\ldots,n\}$: $x[j^*]=0$ et $y[j^*]=1$. Si $\theta[j^*]=0$, alors le bit $v[j^*]$ ne peut prendre aucune valeur et la somme (5.32[102]) est vide; si $\theta[j^*]=1$, alors $v[j^*]$ peut prendre les deux valeurs binaires et dans ce cas

$$v[j^*]=0 \implies v[j^*]\wedge y[j^*]=0,$$

$$v[j^*]=1 \implies v[j^*]\wedge y[j^*]=1,$$

d'où:

$$y\not\preceq x \implies \sum_{\substack{v\ :\ v\oplus x\oplus y\preceq\theta \\ v\preceq\theta\oplus x}} (-1)^{v\odot y} = 0. \quad (5.34)$$

Les lignes (5.33[102]) et (5.34[102]) permettent de continuer le calcul depuis la ligne (5.31[102]):

$$
\begin{aligned}
&= \sum_{\boldsymbol{y} \preceq \boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta} \,\oplus\, \boldsymbol{b}\odot\boldsymbol{x} \,\oplus\, \boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{n+|\boldsymbol{\theta}|+|\boldsymbol{\theta}\oplus\boldsymbol{x}|-2|\boldsymbol{\theta}\wedge\bar{\boldsymbol{x}}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle|\psi_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\rangle \\
&= \sum_{\boldsymbol{y} \preceq \boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta} \,\oplus\, \boldsymbol{b}\odot\boldsymbol{x} \,\oplus\, \boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle|\psi_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\rangle \qquad (5.35) \\
&= \sum_{\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}}}{\sqrt{2}^{n}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle \otimes \sum_{\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{x} \,\oplus\, \boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{|\boldsymbol{x}|}} |\psi_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\rangle \\
&= \sum_{\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}}}{\sqrt{2}^{n}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \qquad (5.36)
\end{aligned}
$$

où la dernière ligne (5.36[103]) est obtenue de la précédente à l'aide de formule de changement de base (5.30[101]), ce qui termine la vérification du circuit de la figure 5.10[100]. ■

Lemme 5.11 (*lemme combinatoire pour* $\mathcal{A}_{n\mathsf{QMC}}$). Considérons un tableau $\boldsymbol{T}$ de 4^n lignes par 3^n colonnes. Les lignes sont indexées par les 4^n paires $(\boldsymbol{\theta},\boldsymbol{b}) \in \{\mathtt{0},\mathtt{1}\}^{2n}$ et les colonnes sont indexées par les 3^n paires $(\boldsymbol{\tau},\boldsymbol{c}) \in \{\mathtt{0},\mathtt{1}\}^{2n}$ telles que $\boldsymbol{c} \preceq \boldsymbol{\tau}$. Soit ℓ tel que $1 \le \ell \le n$. On considère également $\binom{n}{\ell}3^\ell 4^n$ sous-tableaux, tous de dimensions $2^\ell \times 3^{n-\ell}2^\ell$, constitués des cases qui sont à l'intersection de certaines lignes et certaines colonnes de $\boldsymbol{T}$. Les $\binom{n}{\ell}3^\ell 4^n$ sous-tableaux sont en bijection avec les $\binom{n}{\ell}3^\ell 4^n$ choix possibles de valeurs des $3n$ paramètres suivants:

$$
\begin{aligned}
\boldsymbol{r}[1],\ldots,\boldsymbol{r}[n] &\in \{0,1,2,3\}, \\
\boldsymbol{u}[1],\ldots,\boldsymbol{u}[n] &\in \{\mathtt{0},\mathtt{1}\}, \\
\boldsymbol{v}[1],\ldots,\boldsymbol{v}[n] &\in \{\mathtt{0},\mathtt{1}\},
\end{aligned}
$$

soumis à la restriction

$$|\{j \;:\; \boldsymbol{r}[j] \neq 0\}| = \ell. \qquad (5.37)$$

Soient $\boldsymbol{r} \in \{0,1,2,3\}^n$ et $\boldsymbol{u},\boldsymbol{v} \in \{\mathtt{0},\mathtt{1}\}^n$ fixés. La ligne $(\boldsymbol{\theta},\boldsymbol{b})$ fait partie du sous-tableau $(\boldsymbol{r},\boldsymbol{u},\boldsymbol{v})$ selon les conditions suivantes:

$$\forall j \in \{1,\ldots,n\} \ :$$

$$\boldsymbol{r}[j] = 0 \implies (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) \in \{(\boldsymbol{u}[j],\boldsymbol{v}[j])\}, \tag{5.38}$$

$$\boldsymbol{r}[j] = 1 \implies (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) \in \{(\mathtt{1},\boldsymbol{u}[j]),(\mathtt{0},\boldsymbol{v}[j])\}, \tag{5.39}$$

$$\boldsymbol{r}[j] = 2 \implies (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) \in \{(\boldsymbol{u}[j],\mathtt{0}),(\boldsymbol{v}[j],\mathtt{1})\}, \tag{5.40}$$

$$\boldsymbol{r}[j] = 3 \implies (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) \in \{(\boldsymbol{u}[j],\boldsymbol{u}[j]),(\boldsymbol{v}[j],\overline{\boldsymbol{v}[j]})\}. \tag{5.41}$$

La colonne $(\boldsymbol{\tau},\boldsymbol{c})$ fait partie du sous-tableau $(\boldsymbol{r},\boldsymbol{u},\boldsymbol{v})$ selon les conditions suivantes:

$$\forall j \in \{1,\ldots,n\} \ :$$

$$\boldsymbol{r}[j] = 0 \implies (\boldsymbol{\tau}[j],\boldsymbol{c}[j]) \in \{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{0}),(\mathtt{1},\mathtt{1})\}, \tag{5.42}$$

$$\boldsymbol{r}[j] = 1 \implies (\boldsymbol{\tau}[j],\boldsymbol{c}[j]) \in \{(\mathtt{1},\mathtt{0}),(\mathtt{1},\mathtt{1})\}, \tag{5.43}$$

$$\boldsymbol{r}[j] = 2 \implies (\boldsymbol{\tau}[j],\boldsymbol{c}[j]) \in \{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{0})\}, \tag{5.44}$$

$$\boldsymbol{r}[j] = 3 \implies (\boldsymbol{\tau}[j],\boldsymbol{c}[j]) \in \{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{1})\}. \tag{5.45}$$

Alors toute case de $\boldsymbol{T}$ appartient à exactement $\binom{n}{\ell}4^{\ell}$ sous-tableaux.

Preuve. Soit $(\boldsymbol{\theta},\boldsymbol{b},\boldsymbol{\tau},\boldsymbol{c})$, avec $\boldsymbol{c} \preceq \boldsymbol{\tau}$, une case de $\boldsymbol{T}$. Par inspection des conditions (5.38[104]) à (5.45[104]), on établit exhaustivement la liste des triplets $(\boldsymbol{r}[j],\boldsymbol{u}[j],\boldsymbol{v}[j])$ possibles pour $(\boldsymbol{\theta}[j],\boldsymbol{b}[j],\boldsymbol{\tau}[j],\boldsymbol{c}[j])$ fixés, à une position $j \in \{1,\ldots,n\}$ quelconque, voir la figure 5.11[105]. On constate que, pour tout j, tout quadruplet $(\boldsymbol{\theta}[j],\boldsymbol{b}[j],\boldsymbol{\tau}[j],\boldsymbol{c}[j])$ admet exactement un triplet $(\boldsymbol{r}[j],\boldsymbol{u}[j],\boldsymbol{v}[j])$ si $\boldsymbol{r}[j] = 0$, et exactement 4 triplets $(\boldsymbol{r}[j],\boldsymbol{u}[j],\boldsymbol{v}[j])$ si $\boldsymbol{r}[j] \neq 0$. Le lemme découle de cette observation et de la condition (5.37[103]). ■

Remarque 5.12 (*les sous-tableaux du lemme 5.11*[103] *comme f-attaques à* $2n\mathsf{BC}_{\mathsf{H}}$). On peut voir un sous-tableau $(\boldsymbol{r},\boldsymbol{u},\boldsymbol{v})$ de $\boldsymbol{T}$, tel que défini aux lignes (5.38[104])

0000	0010	0011	0100	0110	0111	1000	1010	1011	1100	1110	1111
(0,0,0)	(0,0,0)	(0,0,0)									
			(0,0,1)	(0,0,1)	(0,0,1)						
						(0,1,0)	(0,1,0)	(0,1,0)			
									(0,1,1)	(0,1,1)	(0,1,1)
	(1,0,0)	(1,0,0)					(1,0,0)	(1,0,0)			
				(1,0,1)	(1,0,1)		(1,0,1)	(1,0,1)			
	(1,1,0)	(1,1,0)								(1,1,0)	(1,1,0)
				(1,1,1)	(1,1,1)					(1,1,1)	(1,1,1)
(2,0,0)	(2,0,0)		(2,0,0)	(2,0,0)							
(2,0,1)	(2,0,1)								(2,0,1)	(2,0,1)	
			(2,1,0)	(2,1,0)		(2,1,0)	(2,1,0)				
						(2,1,1)	(2,1,1)		(2,1,1)	(2,1,1)	
(3,0,0)		(3,0,0)	(3,0,0)		(3,0,0)						
(3,0,1)		(3,0,1)				(3,0,1)		(3,0,1)			
			(3,1,0)		(3,1,0)				(3,1,0)		(3,1,0)
						(3,1,1)		(3,1,1)	(3,1,1)		(3,1,1)

FIG. 5.11 – *Lemme combinatoire pour* $\mathcal{A}_{n\mathsf{QMC}}$*: triplets* $(\boldsymbol{r}[j],\boldsymbol{u}[j],\boldsymbol{v}[j])$ *admissibles pour chaque* $(\boldsymbol{\theta}[j],\boldsymbol{b}[j],\boldsymbol{\tau}[j],\boldsymbol{c}[j])$

à (5.45[104]), comme une f-attaque à $2n\mathsf{BC}_\mathsf{H}$ au sens de la définition 4.6[76], en posant $\|\mathbb{Q}_{\boldsymbol{\theta}\oplus\boldsymbol{\tau},\boldsymbol{b}\oplus\boldsymbol{c}}|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2$ comme le contenu de la case $(\boldsymbol{\theta},\boldsymbol{b},\boldsymbol{\tau},\boldsymbol{c})$.

Plus précisément, fixons $(\boldsymbol{r},\boldsymbol{u},\boldsymbol{v}) \in \{0,1,2,3\}^n \times \{\mathtt{0},\mathtt{1}\}^n \times \{\mathtt{0},\mathtt{1}\}^n$ avec

$$|\{j \ : \ \boldsymbol{r}[j] \neq 0\}| = \ell,$$

et soit $f : \{\mathtt{0},\mathtt{1}\}^{2n} \longrightarrow \{\mathtt{0},\mathtt{1}\}^{\ell}$ telle que

$$f(\boldsymbol{\theta},\boldsymbol{b}) \equiv \bigdiamond_{j=1}^{n} \begin{cases} \varepsilon & \text{si } \boldsymbol{r}[j] = 0 \\ \boldsymbol{\theta}[j] & \text{si } \boldsymbol{r}[j] = 1 \\ \boldsymbol{b}[j] & \text{si } \boldsymbol{r}[j] = 2 \\ \boldsymbol{\theta}[j] \oplus \boldsymbol{b}[j] & \text{si } \boldsymbol{r}[j] = 3 \end{cases}.$$

De plus, assignons de façon bijective les 2^ℓ états $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$, définis par les 2^ℓ lignes $(\boldsymbol{\theta},\boldsymbol{b})$ du tableau $(\boldsymbol{r},\boldsymbol{u},\boldsymbol{v})$, à $|\zeta_{\boldsymbol{d}}\rangle$ pour $\boldsymbol{d} \in \{\mathtt{0},\mathtt{1}\}^\ell$ au moyen de la règle suivante:

$$\boldsymbol{d} \equiv \boldsymbol{d}(\boldsymbol{\theta},\boldsymbol{b}) \equiv \bigdiamond_{j=1}^{n} \begin{cases} \varepsilon & \text{si } \boldsymbol{r}[j] = 0 \\ \begin{cases} \mathtt{0} & \text{si } (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) = (\mathtt{1},\boldsymbol{u}[j]) \\ \mathtt{1} & \text{si } (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) = (\mathtt{0},\boldsymbol{v}[j]) \end{cases} & \text{si } \boldsymbol{r}[j] = 1 \\ \begin{cases} \mathtt{0} & \text{si } (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) = (\boldsymbol{u}[j],\mathtt{0}) \\ \mathtt{1} & \text{si } (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) = (\boldsymbol{v}[j],\mathtt{1}) \end{cases} & \text{si } \boldsymbol{r}[j] = 2 \\ \begin{cases} \mathtt{0} & \text{si } (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) = (\boldsymbol{u}[j],\boldsymbol{u}[j]) \\ \mathtt{1} & \text{si } (\boldsymbol{\theta}[j],\boldsymbol{b}[j]) = (\boldsymbol{v}[j],\overline{\boldsymbol{v}[j]}) \end{cases} & \text{si } \boldsymbol{r}[j] = 3 \end{cases}.$$

Alors il est facile de vérifier que toute case $\|\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}|\zeta_{\boldsymbol{d}}\rangle\|^2$ du sous-tableau $(\boldsymbol{r},\boldsymbol{u},\boldsymbol{v})$ est telle que $(\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}) \in f^{-1}(\boldsymbol{d})$.

Autrement dit, *la base est attaquée* aux positions où $\boldsymbol{r}[j] = 1$, *le bit est attaqué* aux positions où $\boldsymbol{r}[j] = 2$, et *le ou exclusif de la base et du bit est attaqué* aux positions où $\boldsymbol{r}[j] = 3$. ▲

Lemme 5.13 (*corollaire du lemme 5.11*[103]). Supposons que chaque case du tableau $\boldsymbol{T}$ contient un nombre réel positif, et soit T le grand total des cases de $\boldsymbol{T}$. Alors il existe un sous-tableau dont la somme des cases est au moins $\frac{T}{3^\ell 4^{n-\ell}}$.

Preuve. La somme de tous les sous-tableaux doit être de $\binom{n}{\ell}4^\ell T$ puisque chaque case appartient à exactement $\binom{n}{\ell}4^\ell$ sous-tableaux. Comme on considère exactement $\binom{n}{\ell}3^\ell 4^n$ sous-tableaux, alors ils ne peuvent pas tous être inférieurs à

$$\frac{\binom{n}{\ell}4^\ell T}{\binom{n}{\ell}3^\ell 4^n} = \frac{T}{3^\ell 4^{n-\ell}}.$$

■

Théorème 5.14 ($\mathcal{A}^1_{2n\mathsf{BC_H}} \leq_\exists \mathcal{A}_{n\mathsf{QMC}}$, *cas parfait*). Soient $\widetilde{C}$ et E deux familles de circuits tels que décrits à la définition 5.8[97] et à la figure 5.9[99], attaquant un $n\mathsf{QMC}$ correspondant à n copies de la figure 5.2[85]. Nous supposons que cette attaque a une ouverture parfaite et un extracteur parfait, c'est-à-dire:

$$\forall\, \boldsymbol{\theta} \in \{+,\times\}^n,\, \boldsymbol{b} \in \{0,1\}^n \;:\; \sum_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}\,:\,\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \|\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 = 1 \tag{5.46}$$

et

$$\forall\, \boldsymbol{\theta} \in \{+,\times\}^n,\, \boldsymbol{b} \in \{0,1\}^n \;:\; |\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \equiv |\|\boldsymbol{b}\|\rangle|\varphi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle. \tag{5.47}$$

Alors il existe une position $j^* \in \{1,\ldots,n\}$ et une f-attaque à $2n\mathsf{BC_H}$ qui est $(\|\widetilde{C}\|_{\mathcal{U}} + \|E\|_{\mathcal{U}},\, \frac{1}{3})$-bonne où f elle l'une des fonctions suivantes:

$$\begin{aligned}
f_{1,j^*} &: \{0,1\}^{2n} \longrightarrow \{0,1\} \;:\; (\boldsymbol{\theta},\boldsymbol{b}) \longmapsto \boldsymbol{\theta}[j^*],\\
f_{2,j^*} &: \{0,1\}^{2n} \longrightarrow \{0,1\} \;:\; (\boldsymbol{\theta},\boldsymbol{b}) \longmapsto \boldsymbol{b}[j^*],\\
f_{3,j^*} &: \{0,1\}^{2n} \longrightarrow \{0,1\} \;:\; (\boldsymbol{\theta},\boldsymbol{b}) \longmapsto \boldsymbol{\theta}[j^*] \oplus \boldsymbol{b}[j^*].
\end{aligned}$$

Preuve. Le lemme 5.10[99] montre qu'il est possible de produire localement chacun des 4^n états $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ comme l'exige la définition 4.6[76].

La preuve du théorème se poursuit par un argument combinatoire qui établit l'existence de deux états, $|\zeta_0\rangle$ et $|\zeta_1\rangle$, parmi $\{|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle : \boldsymbol{\theta} \in \{+,\times\}^n, \boldsymbol{b} \in \{0,1\}^n\}$, qui incarnent une f-attaque à $2n\mathsf{BC}_\mathsf{H}$.

Considérons un tableau $\boldsymbol{T}$ de dimensions $4^n \times 3^n$ où les cases sont indexées par $(\boldsymbol{\theta},\boldsymbol{b},\boldsymbol{\tau},\boldsymbol{c}) \in \{0,1\}^{4n}$ avec $\boldsymbol{c} \preceq \boldsymbol{\tau}$, comme au lemme 5.11[103]. Soit $\|\mathbb{Q}_{\boldsymbol{\theta}\oplus\boldsymbol{\tau},\boldsymbol{b}\oplus\boldsymbol{c}}|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2$ le contenu de la case $(\boldsymbol{\theta},\boldsymbol{b},\boldsymbol{\tau},\boldsymbol{c})$. Par l'hypothèse (5.46[107]), chaque ligne $(\boldsymbol{\theta},\boldsymbol{b})$ de $\boldsymbol{T}$ a un total de 1, et le grand total pour $\boldsymbol{T}$ est de 4^n.

Par les lemmes 5.11[103] et 5.13[107], en posant $\ell \equiv 1$, et par l'hypothèse (5.47[107]), $\boldsymbol{T}$ doit admettre un sous-tableau de dimensions $2 \times 3^{n-1}2$ dont la somme des cases est au moins 4/3. Par les mêmes lemmes, ce sous-tableau est défini par des paramètres $(\boldsymbol{r},\boldsymbol{u},\boldsymbol{v})$ tels que $\boldsymbol{r}[j^*] \neq 0$ pour une unique position j^*. La remarque 5.12[104] donne les deux états $|\zeta_0\rangle$, $|\zeta_1\rangle$ et la f-attaque cherchés, en posant $f \equiv f_{\boldsymbol{r}[j^*],j^*}$. ■

5.3.2.2 Extracteur imparfait

Il est possible d'obtenir une réduction semblable à celle du théorème 5.14[107] dans le cas plus général où l'extracteur de bit de parité E est imparfait, ce qui est démontré au théorème 5.17[114]. La preuve de ce théorème ne peut toutefois faire appel au lemme 5.10[99] puisque ce lemme utilise un extracteur parfait. Afin d'arriver à bon port, nous devons d'abord généraliser la ligne (5.29[101]) ce qui est l'objet du lemme qui suit.

Lemme 5.15 (*propriété d'un extracteur imparfait*). Soient $\widetilde{C}$ et E deux familles de circuits tels que décrits à la définition 5.8[97] et à la figure 5.9[99]. Nous supposons que l'extracteur obtient le bit de parité $\|\boldsymbol{b}\|$ avec un biais moyen $\epsilon \equiv \epsilon(n)$, c'est-à-dire:

$$\frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}} \|\mathbb{P}_{\|\boldsymbol{b}\|}|\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 \geq \frac{1}{2} + \epsilon \tag{5.48}$$

où $\mathbb{P}_{||\boldsymbol{b}||}$ est comme à la ligne (5.25^{98}). Alors on peut écrire

$$\forall \boldsymbol{\theta}, \boldsymbol{b} \ : \ E^\dagger \sigma_z E \ |\vdash\rangle|\boldsymbol{\theta}\rangle|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \ \equiv \ (-1)^{||\boldsymbol{b}||} \ |\boldsymbol{\theta}\rangle \otimes (|\vdash\rangle|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle + \vec{e}_{\boldsymbol{\theta},\boldsymbol{b}}) \tag{5.49}$$

avec

$$\frac{1}{4^n} \sum_{\boldsymbol{\theta},\boldsymbol{b}} ||\vec{e}_{\boldsymbol{\theta},\boldsymbol{b}}||^2 \leq 2 - 4\epsilon. \tag{5.50}$$

Preuve. La ligne (5.48^{108}) décrit la qualité de l'extracteur en moyenne. Cette propriété peut être récrite comme suit:

$$\begin{aligned} E \ |\vdash\rangle|\boldsymbol{\theta}\rangle|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \ &= \ |\boldsymbol{\theta}\rangle \, |\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \\ &\equiv \ |\boldsymbol{\theta}\rangle \otimes (c_{\boldsymbol{\theta},\boldsymbol{b}} |\,||\boldsymbol{b}||\rangle |\varphi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle + \hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} |\overline{||\boldsymbol{b}||}\rangle |\hat{\varphi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle) \end{aligned}$$

où

$$\begin{gathered} c_{\boldsymbol{\theta},\boldsymbol{b}}, \, \hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} \ \in \ [0,1] \subseteq \mathbb{R}, \quad c^2_{\boldsymbol{\theta},\boldsymbol{b}} + \hat{c}^2_{\boldsymbol{\theta},\boldsymbol{b}} = 1, \\ \frac{1}{4^n} \sum_{\boldsymbol{\theta},\boldsymbol{b}} c^2_{\boldsymbol{\theta},\boldsymbol{b}} \geq \frac{1}{2} + \epsilon. \end{gathered} \tag{5.51}$$

Procédons au calcul de $E^\dagger \sigma_z E \ |\vdash\rangle|\boldsymbol{\theta}\rangle|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$:

$$\begin{aligned} &|\vdash\rangle^{\text{Parité}} |\boldsymbol{\theta}\rangle^{\text{Annonces}} |\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle^{\text{Etc}} \\ &\overset{E}{\longmapsto} \ |\boldsymbol{\theta}\rangle \otimes (c_{\boldsymbol{\theta},\boldsymbol{b}} |\,||\boldsymbol{b}||\rangle |\varphi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle + \hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} |\overline{||\boldsymbol{b}||}\rangle |\hat{\varphi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle) \\ &\overset{\sigma_z}{\longmapsto} \ (-1)^{||\boldsymbol{b}||} |\boldsymbol{\theta}\rangle \otimes (c_{\boldsymbol{\theta},\boldsymbol{b}} |\,||\boldsymbol{b}||\rangle |\varphi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle - \hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} |\overline{||\boldsymbol{b}||}\rangle |\hat{\varphi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle) \\ &= \ (-1)^{||\boldsymbol{b}||} |\boldsymbol{\theta}\rangle \otimes (c_{\boldsymbol{\theta},\boldsymbol{b}} |\,||\boldsymbol{b}||\rangle |\varphi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle + \hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} |\overline{||\boldsymbol{b}||}\rangle |\hat{\varphi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle - 2\hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} |\overline{||\boldsymbol{b}||}\rangle |\hat{\varphi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle) \\ &\overset{E^\dagger}{\longmapsto} \ (-1)^{||\boldsymbol{b}||} |\vdash\rangle |\boldsymbol{\theta}\rangle |\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle - 2(-1)^{||\boldsymbol{b}||} \hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} E^\dagger (|\overline{||\boldsymbol{b}||}\rangle |\boldsymbol{\theta}\rangle |\hat{\varphi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle). \end{aligned}$$

On posant

$$|\boldsymbol{\theta}\rangle \otimes \vec{e}_{\boldsymbol{\theta},\boldsymbol{b}} \ \equiv \ -2\hat{c}_{\boldsymbol{\theta},\boldsymbol{b}} E^\dagger (|\overline{||\boldsymbol{b}||}\rangle |\boldsymbol{\theta}\rangle |\hat{\varphi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle)$$

on obtient (5.49[109]). De plus, à l'aide de (5.51[109]):

$$\begin{aligned}\frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}}\|\vec{e}_{\boldsymbol{\theta},\boldsymbol{b}}\|^2 &= \frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}} 4\,\hat{c}^2_{\boldsymbol{\theta},\boldsymbol{b}} \\ &= \frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}} 4(1-c^2_{\boldsymbol{\theta},\boldsymbol{b}}) \\ &\leq 2-4\epsilon,\end{aligned}$$

ce qui montre (5.50[109]). ■

L'étape suivante consiste à généraliser le lemme 5.10[99] au cas de l'extracteur imparfait.

Lemme 5.16 (*circuit de l'attaque pour $\mathcal{A}_{n\mathsf{QMC}}$ avec extracteur imparfait*). Soient $\widetilde{C}$ et E deux familles de circuits tels que décrits à la définition 5.8[97] et à la figure 5.9[99]. On suppose que l'extracteur obtient le bit de parité $\|\boldsymbol{b}\|$ avec un biais moyen $\epsilon \equiv \epsilon(n)$, c'est-à-dire:

$$\frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}}\|\mathbb{P}_{\|\boldsymbol{b}\|}|\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 \geq \frac{1}{2}+\epsilon.$$

Alors on peut préparer 4^n états $\rho_{\boldsymbol{\theta},\boldsymbol{b}}$, pour $\boldsymbol{\theta}\in\{+,\times\}^n$ et $\boldsymbol{b}\in\{\mathtt{0},\mathtt{1}\}^n$, au moyen des portes $\widetilde{C}$ et E sans toucher au registre $\mathcal{H}^{\text{Bob}}$ après qu'un même message quantique de mise en gage soit transmis à Bob, tels que la fidélité moyenne entre $\rho_{\boldsymbol{\theta},\boldsymbol{b}}$ et $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ soit bornée inférieurement par $4\epsilon^2$:

$$\frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}}\langle\psi_{\boldsymbol{\theta},\boldsymbol{b}}|\rho_{\boldsymbol{\theta},\boldsymbol{b}}|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \geq 4\epsilon^2.$$

Preuve. La réduction est la même que celle du lemme 5.10[99] et elle apparaît à la figure 5.10[100]. Les étapes du calcul qui précèdent l'utilisation de l'extracteur sont les mêmes que celles du lemme 5.10[99]. L'état obtenu à cet endroit est équivalent à celui de la ligne (5.35[103]) auquel on aura appliqué les portes $E^\dagger_{\text{Parfait}}\sigma_z^\dagger E_{\text{Parfait}} = E^\dagger_{\text{Parfait}}\sigma_z E_{\text{Parfait}}$ où E_{Parfait} est un extracteur parfait:

$$|\vdash\rangle^{\text{Etc}}|\Phi_n^+\rangle^{\text{Annonces,Qubits}}$$

$$\overset{T^{\otimes\boldsymbol{\theta}}B^{\otimes\boldsymbol{b}}\widetilde{C}}{\longmapsto} \quad \sum_{\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{y}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{b}\,\oplus\,\boldsymbol{y}\odot\boldsymbol{y}}}{\sqrt{2}^{n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle|\psi_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\rangle,$$

d'où on continue à l'aide du lemme 5.15[108]:

$$\overset{E^{\dagger}\sigma_z E}{\longmapsto} \quad \sum_{\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle\otimes(|\vdash\rangle|\psi_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\rangle+\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}). \tag{5.52}$$

Scindons la somme (5.52[111]) en deux:

$$|\hat{\Psi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle = |\Psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle + \vec{F}_{\boldsymbol{\theta},\boldsymbol{b}}$$

où

$$\begin{aligned}
|\hat{\Psi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle &\equiv \sum_{\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle\otimes(|\vdash\rangle|\psi_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\rangle+\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}),\\
|\Psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle &\equiv \sum_{\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{n+|\boldsymbol{x}|}} |\vdash\rangle|\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle|\psi_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\rangle,\\
\vec{F}_{\boldsymbol{\theta},\boldsymbol{b}} &\equiv \sum_{\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle\otimes\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}.
\end{aligned}$$

Le premier morceau $|\Psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ est identique à l'état obtenu à la ligne (5.35[103]) avec un extracteur parfait. Il peut donc être récrit à l'aide de la ligne (5.36[103]):

$$|\Psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle = \sum_{\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}}}{\sqrt{2}^{n}} |\vdash\rangle|\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle. \tag{5.53}$$

Tâchons maintenant de borner l'erreur moyenne commise par l'utilisation d'un extracteur imparfait:

$$\begin{aligned}
&\frac{1}{4^n}\sum_{\boldsymbol{b},\boldsymbol{\theta}} \|\vec{F}_{\boldsymbol{\theta},\boldsymbol{b}}\|^2\\
&= \sum_{\boldsymbol{b},\boldsymbol{\theta}} \Big\|\sum_{\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{3n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle\otimes\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\Big\|^2\\
&= \sum_{\boldsymbol{b},\boldsymbol{\theta}} \Big\|\sum_{\boldsymbol{x}} \sum_{\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{y}}}{\sqrt{2}^{3n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle\otimes\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\Big\|^2\\
&= \sum_{\boldsymbol{b},\boldsymbol{\theta}} \Big\|\sum_{\boldsymbol{x}} \frac{(-1)^{\boldsymbol{b}\odot\boldsymbol{\theta}\,\oplus\,\boldsymbol{b}\odot\boldsymbol{x}}}{\sqrt{2}^{3n+|\boldsymbol{x}|}} |\boldsymbol{\theta}\oplus\boldsymbol{x}\rangle\otimes \sum_{\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}} (-1)^{\boldsymbol{b}\odot\boldsymbol{y}}\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\Big\|^2
\end{aligned}$$

$$= \sum_{\boldsymbol{b},\boldsymbol{\theta},\boldsymbol{x}} \frac{1}{2^{3n+|\boldsymbol{x}|}} \| \sum_{\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}} (-1)^{\boldsymbol{b}\odot\boldsymbol{y}} \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}} \|^2 \tag{5.54}$$

$$= \sum_{\boldsymbol{\theta},\boldsymbol{x}} \frac{1}{2^{3n+|\boldsymbol{x}|}} \sum_{\boldsymbol{b}} \| \sum_{\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}} (-1)^{\boldsymbol{b}\odot\boldsymbol{y}} \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}} \|^2 \tag{5.55}$$

où la ligne (5.54[112]) est obtenue par le théorème de Pythagore appliqué à la somme sur les $\boldsymbol{x}$ dont les termes sont orthogonaux deux à deux.

On doit simplifier la ligne (5.55[112]) en invoquant l'identité du parallélogramme généralisée. Soient $\boldsymbol{\theta}$ et $\boldsymbol{x}$ fixés, soient

$$\begin{aligned}
\boldsymbol{w} &\equiv \boldsymbol{b} \\
\boldsymbol{z} &\equiv \boldsymbol{y} \\
A &\equiv \{\boldsymbol{y} \in \{0,1\}^n \;:\; \boldsymbol{y} \preceq \boldsymbol{x}\} \\
\vec{v}_{\boldsymbol{w},\boldsymbol{z}} &\equiv \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}},
\end{aligned}$$

soient $\boldsymbol{s},\boldsymbol{t} \in \{0,1\}^n$ tels que $\boldsymbol{s} \neq \boldsymbol{t}$ et vérifions la condition (2.25[45]) du lemme 2.33[45]:

$$\begin{aligned}
&\sum_{\boldsymbol{w}} \sum_{z_1\in A:\boldsymbol{w}\oplus z_1=\boldsymbol{s}} \sum_{z_2\in A:\boldsymbol{w}\oplus z_2=\boldsymbol{t}} (-1)^{\boldsymbol{w}\odot(z_1\oplus z_2)} \langle \vec{v}_{\boldsymbol{w},z_1}, \vec{v}_{\boldsymbol{w},z_2} \rangle \\
&= \sum_{\boldsymbol{b}} \sum_{y_1\in A:\boldsymbol{b}\oplus y_1=\boldsymbol{s}} \sum_{y_2\in A:\boldsymbol{b}\oplus y_2=\boldsymbol{t}} (-1)^{\boldsymbol{b}\odot(y_1\oplus y_2)} \langle \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus y_1}, \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus y_2} \rangle \\
&= \sum_{\boldsymbol{b}} \sum_{y_1\in A:\boldsymbol{b}\oplus y_1=\boldsymbol{s}} \sum_{y_2\in A:\boldsymbol{b}\oplus y_2=\boldsymbol{t}} (-1)^{\boldsymbol{b}\odot(\boldsymbol{s}\oplus\boldsymbol{t})} \langle \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{s}}, \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{t}} \rangle \\
&= \langle \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{s}}, \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{t}} \rangle \sum_{\boldsymbol{b}} (-1)^{\boldsymbol{b}\odot(\boldsymbol{s}\oplus\boldsymbol{t})} \sum_{y_1\in A:\boldsymbol{b}\oplus y_1=\boldsymbol{s}} \sum_{y_2\in A:\boldsymbol{b}\oplus y_2=\boldsymbol{t}} 1 \\
&= \langle \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{s}}, \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{t}} \rangle \sum_{\boldsymbol{b}\,:\,\boldsymbol{b}\oplus\boldsymbol{s}\preceq\boldsymbol{x} \text{ et } \boldsymbol{b}\oplus\boldsymbol{t}\preceq\boldsymbol{x}} (-1)^{\boldsymbol{b}\odot(\boldsymbol{s}\oplus\boldsymbol{t})} &(5.56) \\
&= \langle \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{s}}, \vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{t}} \rangle \, 0 &(5.57) \\
&= 0.
\end{aligned}$$

La ligne (5.57[112]) s'obtient de la précédente comme ceci: à la position j^* où $\boldsymbol{s}[j^*] \neq \boldsymbol{t}[j^*]$, si $\boldsymbol{x}[j^*] = 0$ alors la somme (5.56[112]) est vide; si $\boldsymbol{x}[j^*] = 1$ alors $\boldsymbol{b}[j^*]$ peut prendre les deux valeurs binaires et dans ce cas $\boldsymbol{b}[j^*] = 0 \Rightarrow \boldsymbol{b}[j^*] \wedge (\boldsymbol{s}[j^*] \oplus \boldsymbol{t}[j^*]) = 0$ et $\boldsymbol{b}[j^*] = 1 \Rightarrow \boldsymbol{b}[j^*] \wedge (\boldsymbol{s}[j^*] \oplus \boldsymbol{t}[j^*]) = 1$ ce qui rend la somme totale nulle.

Les conditions du lemme 2.33[45] ont été vérifiées alors on peut en écrire la conclusion:

$$\begin{aligned} & \sum_{\boldsymbol{w}} \|\sum_{\boldsymbol{z}\in A}(-1)^{\boldsymbol{w}\odot\boldsymbol{z}}\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2 &=& \sum_{\boldsymbol{w}\in\{0,1\}^n,\boldsymbol{z}\in A}\|\vec{v}_{\boldsymbol{w},\boldsymbol{z}}\|^2 \\ \Longleftrightarrow \quad & \sum_{\boldsymbol{b}}\|\sum_{\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}}(-1)^{\boldsymbol{b}\odot\boldsymbol{y}}\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\|^2 &=& \sum_{\boldsymbol{b},\,\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}}\|\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\|^2, \end{aligned}$$

ce qui permet de simplifier la ligne (5.55[112]) comme suit:

$$\begin{aligned} &= \sum_{\boldsymbol{\theta},\boldsymbol{x}}\frac{1}{2^{3n+|\boldsymbol{x}|}}\sum_{\boldsymbol{b},\,\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}}\|\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\|^2 \\ &= \sum_{\boldsymbol{x},\,\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}}\frac{1}{2^{3n+|\boldsymbol{x}|}}\sum_{\boldsymbol{\theta},\boldsymbol{b}}\|\vec{e}_{\boldsymbol{\theta}\oplus\boldsymbol{x},\boldsymbol{b}\oplus\boldsymbol{y}}\|^2 \\ &\leq \sum_{\boldsymbol{x},\,\boldsymbol{y}\,:\,\boldsymbol{y}\preceq\boldsymbol{x}}\frac{1}{2^{3n+|\boldsymbol{x}|}}4^n(2-4\epsilon) \qquad (5.58) \\ &= 2-4\epsilon, \end{aligned}$$

où la ligne (5.58[113]) est obtenue à l'aide de la ligne (5.50[109]) du lemme 5.15[108].

On a donc prouvé la borne

$$\frac{1}{4^n}\sum_{\boldsymbol{b},\boldsymbol{\theta}}\|\vec{F}_{\boldsymbol{\theta},\boldsymbol{b}}\|^2 \leq 2-4\epsilon. \qquad (5.59)$$

Nous allons utiliser (5.59[113]) pour borner inférieurement la fidélité moyenne entre $|\Psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ et $|\hat{\Psi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$:

$$\begin{aligned} \frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}}|\langle\Psi_{\boldsymbol{\theta},\boldsymbol{b}}|\hat{\Psi}_{\boldsymbol{\theta},\boldsymbol{b}}\rangle|^2 &\geq \frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}}(1-\frac{\|\vec{F}_{\boldsymbol{\theta},\boldsymbol{b}}\|^2}{2})^2 \qquad (5.60) \\ &\geq (1-\frac{1}{2\ 4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}}\|\vec{F}_{\boldsymbol{\theta},\boldsymbol{b}}\|^2)^2 \qquad (5.61) \\ &\geq (1-\frac{1}{2}(2-4\epsilon))^2 \qquad (5.62) \end{aligned}$$

$$= \quad 4\epsilon^2.$$

La ligne (5.60[113]) s'obtient avec la proposition 2.23[32], la ligne (5.61[113]) est due au fait que la fonction $x \mapsto (1 - \frac{x}{2})^2$ est convexe, et la ligne (5.62[113]) utilise l'inégalité (5.59[113]).

De cette dernière borne, de l'identité (5.53[111]) et de la proposition 2.21[32] découle l'énoncé du présent lemme. ■

Nous sommes maintenant outillés pour affronter le théorème 5.17[114], généralisation du théorème 5.14[107] au cas de l'extracteur imparfait.

Théorème 5.17 ($\mathcal{A}^{\ell}_{2n\mathsf{BC_H}} \leq_{\exists} \mathcal{A}_{n\mathsf{QMC}}$, *ouverture parfaite et extracteur imparfait*). Soient $\widetilde{C}$ et E deux familles de circuits tels que décrits à la définition 5.8[97] et à la figure 5.9[99], attaquant un $n\mathsf{QMC}$ correspondant à n copies de la figure 5.2[85]. Nous supposons que cette attaque a une ouverture parfaite:

$$\forall\, \boldsymbol{\theta} \in \{+,\times\}^n,\ \boldsymbol{b} \in \{\mathtt{0},\mathtt{1}\}^n \ : \sum_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}\ :\ \boldsymbol{b}\oplus\hat{\boldsymbol{b}} \preceq \boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \|\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}} |\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 = 1, \tag{5.63}$$

et que l'extracteur est $\epsilon \equiv \epsilon(n)$-bon pour $\epsilon(n) \notin \mathrm{negl}(n)$:

$$\frac{1}{4^n} \sum_{\boldsymbol{\theta},\boldsymbol{b}} \|\mathbb{P}_{\|\boldsymbol{b}\|} |\phi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 \geq \frac{1}{2} + \epsilon(n).$$

Si $\eta \equiv \eta(n) \notin \mathrm{negl}(n)$ et si

$$\ell \equiv \ell(n) \equiv \left\lceil \log_{\frac{4}{3}} \left(\frac{1 + \eta(n)}{4\epsilon(n)^2} \right) \right\rceil,$$

alors il existe une f-attaque à $2n\mathsf{BC_H}$ avec

$$f \ : \ \{\mathtt{0},\mathtt{1}\}^{2n} \longrightarrow \{\mathtt{0},\mathtt{1}\}^{\ell}$$

qui est $(\|\widetilde{C}\|_{\mathcal{U}} + \|E\|_{\mathcal{U}}, \eta(n))$-bonne, voir la définition 4.6[76].

Preuve. Le lemme 5.16[110] montre qu'il est possible de produire localement une famille de 4^n états $\rho_{\boldsymbol{\theta},\boldsymbol{b}}$ qui sont tels que la fidélité moyenne de $\rho_{\boldsymbol{\theta},\boldsymbol{b}}$ à $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ est au moins $4\epsilon^2$:

$$\frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}}\langle\psi_{\boldsymbol{\theta},\boldsymbol{b}}|\rho_{\boldsymbol{\theta},\boldsymbol{b}}|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \geq 4\epsilon^2. \tag{5.64}$$

Comme pour le théorème 5.14[107], la suite de l'argumentation est combinatoire et fait appel aux lemmes 5.11[103] et 5.13[107] et à la remarque 5.12[104].

Considérons un tableau $\boldsymbol{T}$ de dimensions $4^n \times 3^n$ où les cases sont indexées par $(\boldsymbol{\theta},\boldsymbol{b},\boldsymbol{\tau},\boldsymbol{c}) \in \{0,1\}^{4n}$ avec $\boldsymbol{c} \preceq \boldsymbol{\tau}$, comme au lemme 5.11[103]. Soit $\mathrm{tr}(\mathbb{Q}_{\boldsymbol{\theta}\oplus\boldsymbol{\tau},\boldsymbol{b}\oplus\boldsymbol{c}}\rho_{\boldsymbol{\theta},\boldsymbol{b}})$ le contenu de la case $(\boldsymbol{\theta},\boldsymbol{b},\boldsymbol{\tau},\boldsymbol{c})$, c'est-à-dire la probabilité d'observer le résultat associé au projecteur $\mathbb{Q}_{\boldsymbol{\theta}\oplus\boldsymbol{\tau},\boldsymbol{b}\oplus\boldsymbol{c}}$ étant donnée la préparation $\rho_{\boldsymbol{\theta},\boldsymbol{b}}$. Bornons inférieurement le grand total T des cases de $\boldsymbol{T}$:

$$\begin{aligned}
T &\equiv \sum_{\boldsymbol{\theta},\boldsymbol{b},\boldsymbol{\tau},\boldsymbol{c}:\boldsymbol{c}\preceq\boldsymbol{\tau}} \mathrm{tr}(\mathbb{Q}_{\boldsymbol{\theta}\oplus\boldsymbol{\tau},\boldsymbol{b}\oplus\boldsymbol{c}}\rho_{\boldsymbol{\theta},\boldsymbol{b}}) \\
&= \sum_{\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \mathrm{tr}(\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}\rho_{\boldsymbol{\theta},\boldsymbol{b}}) \\
&= \sum_{\boldsymbol{\theta},\boldsymbol{b}} \mathrm{tr}\big(\big(\sum_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}\,:\,\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}\big)\rho_{\boldsymbol{\theta},\boldsymbol{b}}\big) \\
&\geq \sum_{\boldsymbol{\theta},\boldsymbol{b}}\langle\psi_{\boldsymbol{\theta},\boldsymbol{b}}|\rho_{\boldsymbol{\theta},\boldsymbol{b}}|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle \qquad (5.65) \\
&\geq 4^{n+1}\epsilon^2. \qquad (5.66)
\end{aligned}$$

La ligne (5.65[115]) s'obtient avec la proposition 2.20[31] et en observant, depuis (5.63[114]), que

$$\forall\, \boldsymbol{\theta},\boldsymbol{b} \;:\; \|\big(\sum_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}\,:\,\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}\big)|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle\|^2 = 1$$

car les projecteurs $\mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}$ sont orthogonaux deux à deux, voir la proposition 2.22[32]. La ligne (5.66[115]) découle facilement de (5.65[115]) et (5.64[115]).

Invoquons maintenant les lemmes 5.11[103] et 5.13[107] pour conclure que $\boldsymbol{T}$ admet un sous-tableau de dimensions $2^\ell \times 3^{n-\ell}2^\ell$ dont la somme des cases est au moins

$$\begin{aligned} \frac{T}{3^\ell 4^{n-\ell}} &\geq \frac{4^{n+1}\epsilon^2}{3^\ell 4^{n-\ell}} \\ &= 4\epsilon^2(\frac{4}{3})^\ell \\ &\geq 1+\eta. \end{aligned}$$

Suivant l'interprétation de la remarque 5.12[104] et la définition 4.6[76], nous sommes en présence de la f-attaque cherchée. ■

Deux remarques sur le théorème 5.17[114] permettront d'en apprécier la portée. Tout d'abord, si l'on pose $\epsilon = \frac{1}{2}$ et $\eta = \frac{1}{3}$, alors on a démontré de nouveau le théorème 5.14[107]. Ensuite, si $\eta(n) \notin \mathrm{negl}(n)$ alors $\ell(n) \in \mathrm{polylog}(n)$, c'est-à-dire: si on désire une attaque de qualité au moins non négligeable $\eta(n)$ sur $2n\mathsf{BC}_\mathsf{H}$, alors on doit f-attaquer $\ell(n)$ bits parmi $2n$ bits, mais heureusement pas plus qu'une quantité polylogarithmique en n, comme nous l'a autorisé la remarque 4.7[77].

5.3.2.3 Ouverture imparfaite et extracteur imparfait

Ce cas, encore plus général que celui de la section précédente, ne sera pas couvert formellement et fera l'objet d'un commentaire au chapitre 6 (problème P7[124]).

Que peut-on obtenir d'un adversaire $\mathcal{A}_{n\mathsf{QMC}}$ qui ne peut réussir le test de la ligne (5.22[97]) qu'avec probabilité moyenne $\delta(n)$ et ne peut extraire le bit de parité qu'avec un biais moyen $\epsilon(n)$? Si l'on souhaite conserver l'approche de la preuve du théorème 5.17[114], alors on devra d'abord généraliser la proposition 2.20[31]. En effet, cette proposition est nécessaire pour obtenir la ligne (5.65[115]). Mais si l'ouverture est imparfaite, alors $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ n'est plus un vecteur propre du projecteur

$$\sum_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}\,:\,\boldsymbol{b}\oplus\hat{\boldsymbol{b}}\preceq\boldsymbol{\theta}\oplus\hat{\boldsymbol{\theta}}} \mathbb{Q}_{\hat{\boldsymbol{\theta}},\hat{\boldsymbol{b}}}$$

et la proposition 2.20[31] ne peut plus être invoquée telle quelle. Ensuite, il faudra s'assurer que le grand total du tableau $\boldsymbol{T}$ des théorèmes 5.14[107] ou 5.17[114] est suffisamment grand pour qu'on puisse y dénicher une f-attaque décente à $2n\mathsf{BC}_{\mathsf{H}}$.

Remarquons que les lemmes 5.11[103] et 5.13[107], de même que la remarque 5.12[104], sont purement combinatoires et ne dépendent d'aucune hypothèse sur l'ouverture ou l'extracteur et ils pourraient être invoqués de nouveau. Les lemmes 5.15[108] et 5.16[110] seraient également recyclables car ils ne dépendent d'aucune hypothèse à propos de l'ouverture.

5.3.3 Du protocole de transfert inconscient à la mise en gage de mesure

Dans cette section, nous analysons le lien qui doit être établi entre la sécurité du protocole de transfert inconscient et la mise en gage de mesure. Nous abandonnons le strict formalisme des sections précédentes: on évite ainsi une certaine redondance dans les définitions et les énoncés des théorèmes sans compromettre la clarté du discours. Le lecteur pourra sans difficulté reconstituer des définitions et des preuves formelles en s'inspirant de celles de la section 5.3.2[96].

Nous divisons notre analyse en deux segments

$$\mathsf{OT}_{\mathsf{S}} \longrightarrow n\mathsf{QMC}_{\text{Partiel}} \quad \text{et} \quad n\mathsf{QMC}_{\text{Partiel}} \longrightarrow n\mathsf{QMC}$$

où $n\mathsf{QMC}_{\text{Partiel}}$ est une primitive accessoire introduite dans la sous-section qui suit.

5.3.3.1 $n\mathsf{QMC}_{\text{Partiel}} \longrightarrow n\mathsf{QMC}$

Le modèle étudié à la section 5.3.2[96] ne correspond pas tout à fait à un adversaire à OT_{S} tenant le rôle d'Alice dans le protocole de la figure 5.1[80]. En effet, un tel adversaire se doit d'obtenir de l'information qui soit corrélée à plus d'un des deux bits secrets a_0 et a_1. Pour ce faire, il doit tenter d'extraire les bits de parité de deux sous-chaînes de $\boldsymbol{b}$. Pour cette raison, nous considérons maintenant une mise en gage de mesure dont la notion d'adversaire est encore une paire *mise en gage–extracteur*, mais ici l'extracteur tente d'obtenir la parité de deux sous-chaînes de $\boldsymbol{b}$ de longueur $\frac{n}{3}$ après une mise en gage des mesures sur les n qubits BB84 $|\boldsymbol{b}\rangle_{\boldsymbol{\theta}}$. Appelons un tel extracteur un *extracteur partiel*, E_{Partiel}, et notons la primitive par $n\mathsf{QMC}_{\text{Partiel}}$.

La réduction que nous tentons d'établir est la suivante:

$$\mathcal{A}_{n\mathsf{QMC}} \leq_{\exists} \mathcal{A}_{n\mathsf{QMC}_{\text{Partiel}}}, \tag{5.67}$$

et nous en présentons les grandes lignes.

On suppose que E_{Partiel} tente d'obtenir les bits

$$\begin{aligned} \|\boldsymbol{b}\|_{I_0} &\equiv \bigoplus_{j\in I_0} \boldsymbol{b}[j] \\ \|\boldsymbol{b}\|_{I_1} &\equiv \bigoplus_{j\in I_1} \boldsymbol{b}[j] \end{aligned}$$

où $I_0 \equiv I_0(n) \equiv \{1,\ldots,\frac{n}{3}\}$ et $I_1 \equiv I_1(n) \equiv \{\frac{n}{3}+1,\ldots,\frac{2n}{3}\}$. Paramétrons la qualité de cette extraction:

Définition 5.18 (*qualité d'un extracteur partiel*). Un extracteur partiel E_{Partiel} tel que décrit ci-dessus est $\lambda(n)$-bon si $\lambda(n)$ est une borne inférieure sur la moyenne, lorsque $\boldsymbol{b}$ et $\boldsymbol{\theta}$ sont uniformément choisis au hasard, du minimum entre les biais $\lambda_{I_0,\boldsymbol{\theta},\boldsymbol{b}}$ et $\lambda_{I_1,\boldsymbol{\theta},\boldsymbol{b}}$ en faveur des bits $\|\boldsymbol{b}\|_{I_0}$ et $\|\boldsymbol{b}\|_{I_1}$ respectivement, étant donnés les qubits $|\boldsymbol{b}\rangle_{\boldsymbol{\theta}}$:

$$\lambda_{\boldsymbol{\theta},\boldsymbol{b}} \equiv \min(\lambda_{I_0,\boldsymbol{\theta},\boldsymbol{b}}, \lambda_{I_1,\boldsymbol{\theta},\boldsymbol{b}})$$
$$\frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}} \lambda_{\boldsymbol{\theta},\boldsymbol{b}} \geq \lambda(n).$$

▲

Rappelons que le *biais* est $\frac{1}{2}$ de moins que la probabilité d'observer le bit désiré.

L'idée de base de la réduction consiste à se servir de l'extracteur E_{Partiel} sur $3n$ qubits BB84 en ajoutant accessoirement $2n$ qubits aux n déjà présents. On obtient ainsi le bit de parité de $\boldsymbol{b}$ comme premier élément de la paire retournée par E_{Partiel}. La composante de mise en gage $\widetilde{C}$ de la réduction demeure la même d'un adversaire à l'autre.

Théorème 5.19 ($E \leq_\exists E_{\text{Partiel}}$). Soit E_{Partiel} un extracteur partiel $\lambda(n)$-bon, comme à la définition 5.18[118]. Soit $\boldsymbol{\xi} \equiv \boldsymbol{\xi}_n \in \{+,\times\}^{2n}$ et $\boldsymbol{x} \equiv \boldsymbol{x}_n \in \{0,1\}^{2n}$ deux familles de chaînes de bits qui sont telles que E_{Partiel} est au moins aussi bon lorsque $2n$ qubits sur $3n$ sont fixés à $|\boldsymbol{x}\rangle_{\boldsymbol{\xi}}$, plus précisément:

$$\frac{1}{4^n} \sum_{\substack{\boldsymbol{\theta}\in\{+,\times\}^n \\ \boldsymbol{b}\in\{0,1\}^n}} \lambda_{(\boldsymbol{\theta},\boldsymbol{\xi}),(\boldsymbol{b},\boldsymbol{x})} \quad \geq \quad \frac{1}{4^{3n}} \sum_{\substack{\boldsymbol{\theta}\in\{+,\times\}^{3n} \\ \boldsymbol{b}\in\{0,1\}^{3n}}} \lambda_{\boldsymbol{\theta},\boldsymbol{b}} \quad \geq \quad \lambda(3n). \tag{5.68}$$

Soit E l'extracteur construit à partir de E_{Partiel} comme au paragraphe précédent. Alors E sera $\lambda(3n)$-bon, voir la définition 5.8[97].

Preuve. Fixons $\boldsymbol{\theta} \in \{+,\times\}^n$ et $\boldsymbol{b} \in \{0,1\}^n$ et notons:

$$\lambda'_0 \equiv \lambda_{I_0(3n),(\boldsymbol{\theta},\boldsymbol{\xi}),(\boldsymbol{b},\boldsymbol{x})}, \quad \lambda'_1 \equiv \lambda_{I_1(3n),(\boldsymbol{\theta},\boldsymbol{\xi}),(\boldsymbol{b},\boldsymbol{x})},$$

$$\lambda' \equiv \min(\lambda'_0, \lambda'_1) = \lambda_{(\boldsymbol{\theta},\boldsymbol{\xi}),(\boldsymbol{b},\boldsymbol{x})}.$$

La probabilité $p_{\boldsymbol{\theta},\boldsymbol{b}}$ que E calcule correctement le bit $\|\boldsymbol{b}\|$ est égale à la probabilité que E_{Partiel} retourne $\|\boldsymbol{b}\|$ comme première composante, d'où

$$\begin{aligned} p_{\boldsymbol{\theta},\boldsymbol{b}} &= \frac{1}{2} + \lambda'_0 \\ &\geq \frac{1}{2} + \lambda'. \end{aligned}$$

Le biais $\epsilon_{\boldsymbol{\theta},\boldsymbol{b}}$ obtenu par E en $(\boldsymbol{\theta},\boldsymbol{b})$ est donc

$$\epsilon_{\boldsymbol{\theta},\boldsymbol{b}} = p_{\boldsymbol{\theta},\boldsymbol{b}} - \frac{1}{2}$$

$$
\begin{aligned}
&\geq \lambda' \\
&= \lambda_{(\boldsymbol{\theta},\boldsymbol{\xi}),(\boldsymbol{b},\boldsymbol{x})}.
\end{aligned}
$$

Le passage à la moyenne se fait aisément:

$$
\begin{aligned}
\frac{1}{4^n}\sum_{\substack{\boldsymbol{\theta}\in\{+,\times\}^n\\ \boldsymbol{b}\in\{0,1\}^n}} \epsilon_{\boldsymbol{\theta},\boldsymbol{b}} &\geq \frac{1}{4^n}\sum_{\boldsymbol{\theta},\boldsymbol{b}} \lambda_{(\boldsymbol{\theta},\boldsymbol{\xi}),(\boldsymbol{b},\boldsymbol{x})} \\
&\geq \lambda(3n), \qquad (5.69)
\end{aligned}
$$

où la ligne (5.69[120]) vient de (5.68[119]). ■

Techniquement, la réduction du théorème 5.19[119] est non uniforme à cause des chaînes $\boldsymbol{\xi}$ et $\boldsymbol{x}$ qui doivent exister, mais pour lesquelles nous ne donnons aucune construction explicite.

Nous omettons les derniers détails qui mèneraient à une preuve complète et formelle de la réduction (5.67[118]) qui tiendrait compte de la mise en gage $\widetilde{C}$ aussi bien que de l'extracteur, de même que des pertes en temps de calcul et en probabilité de succès montrées au théorème 5.19[119]. L'énoncé du théorème nous indique que ces pertes sont raisonnables, c'est-à-dire qu'une probabilité de succès non négligeable reste non négligeable après réduction, et un temps de calcul polynômial demeure polynômial.

5.3.3.2 $\mathsf{OT}_\mathsf{S} \longrightarrow n\mathsf{QMC}_{\text{Partiel}}$

Pour ce dernier segment, nous devons étudier une réduction

$$\mathcal{A}_{n\mathsf{QMC}_{\text{Partiel}}} \leq_\exists \mathcal{A}_{\mathsf{OT}_\mathsf{S}}. \qquad (5.70)$$

Nous ne donnons pas de détails formels, mais nous traçons clairement la voie à suivre afin que le lecteur suffisamment méticuleux puisse les écrire sans grande difficulté. Nous l'invitons à relire les deux premiers paragraphes de la section 5.3[83].

La différence entre un adversaire au protocole de transfert inconscient et un adversaire à une mise en gage de mesure réside essentiellement dans le rôle des mises en gage. Dans le protocole décrit à la section 5.1[79], $2n$ positions sont mises en gage dont n sont sacrifiées et ouvertes afin de tester la probité d'Alice. Les autres positions pourraient ne jamais être ouvertes, du moins pas tant que le protocole est en cours. C'est sur ces positions non ouvertes que l'adversaire tentera d'extraire des bits de parité. Par contraste, dans une mise en gage de mesure, il n'y a pas de positions *ouvertes* ou *non ouvertes*. L'extraction a lieu sur les mêmes n positions qui servent au test.

De ce point de vue, un adversaire au protocole $\mathsf{OT_S}$ de la section 5.1[79] est aussi une paire *mise en gage–extracteur*, mais sa qualité doit être décrite par la probabilité de réussir un test d'ouverture exécuté sur la moitié des positions choisies uniformément au hasard et par les biais obtenus en faveur de bits de parité sur les autres positions. Dans une réduction comme à la ligne (5.70[120]), un adversaire $\mathcal{A}_{\mathsf{OT_S}}$ sera recyclé sans modification pour construire un attaquant $\mathcal{A}_{n\mathsf{QMC}_{\text{Partiel}}}$ en permettant toutefois à l'extracteur E_{Partiel} de choisir — de façon non uniforme — les positions sur lesquelles il désire obtenir les bits de parités. Les adversaires $\mathcal{A}_{n\mathsf{QMC}_{\text{Partiel}}}$ et $\mathcal{A}_{\mathsf{OT_S}}$ se distinguent uniquement par la façon dont on définit la qualité, et non pas par le format du circuit.

Le reste de l'analyse consiste à trouver deux bornes. Il faut borner inférieurement la probabilité de succès à l'ouverture de $\mathcal{A}_{n\mathsf{QMC}_{\text{Partiel}}}$ étant donnée une probabilité de succès à l'ouverture de $\mathcal{A}_{\mathsf{OT_S}}$. En tenant compte du fait que le test d'ouverture de $\mathcal{A}_{\mathsf{OT_S}}$ porte sur la moitié des positions choisies uniformément au hasard, on montrera que la probabilité de succès du test à l'ouverture de toutes les positions ne peut dégringoler du non négligeable au négligeable. Entre autres, on se convaincra assez facilement que si $\mathcal{A}_{\mathsf{OT_S}}$ a une ouverture parfaite, alors $\mathcal{A}_{n\mathsf{QMC}_{\text{Partiel}}}$ en aura une aussi. D'autre part, il faut borner inférieurement la qualité de E_{Partiel}, telle que définie à la définition 5.18[118], étant donnée la qualité d'un extracteur $E_{\mathsf{OT_S}}$

définie semblablement. Cette tâche n'est pas ardue et n'implique qu'une analyse semblable à celle de la section 5.3.3.1[117].

Chapitre 6

Conclusions et avenues de recherche

Il est temps de prendre un peu de recul, de méditer sur le travail accompli et sur celui qui reste à faire.

Nous invitons le lecteur à consulter le tableau synoptique des figures 6.1[124] et 6.2[125] tout au long de ce chapitre. On y a rassemblé les problèmes non résolus par cette thèse de même que les principales avenues de recherche que nous proposons. Un indice de difficulté apparaît en dernière colonne. Il est emprunté à Knuth [Knu73]. Il s'agit d'une échelle "logarithmique" de 0 à 50 qui prend la signification suivante:

- 0 : immédiat,
- 10 : simple, une minute de travail,
- 20 : intermédiaire, un quart d'heure de travail,
- 30 : modérément difficile,
- 40 : travail de session,
- 50 : problème de recherche.

La première colonne contient un numéro auquel nous nous référerons dans le texte.

	Sujet	Problème	Cote
P1.	$\mathsf{BC_H} \leq \mathsf{QOWP}$	Trouver une réduction aussi simple vers une hypothèse moins forte.	50
P2.	$\mathsf{BC_H} \leq \mathsf{QOWP}$	Considérer un modèle de canal quantique avec erreurs.	45
P3.	$\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}^1_{m\mathsf{BC_H}}$	Donner les détails de cette généralisation de $\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC_H}}$.	35
P4.	$\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}^\ell_{m\mathsf{BC_H}}$	Soit $\ell \in \mathrm{polylog}(m)$. Généraliser $\mathsf{BC_H} \leq \mathsf{QOWP}$ à la mise en gage de chaînes de bits, et généraliser $\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC_H}}$ aux f-attaques sur m bits.	50
P5.	$\mathcal{A}^1_{m\mathsf{BC_H}} \leq_\exists \mathcal{A}^\ell_{m\mathsf{BC_H}}$	Soit $\ell \in \mathrm{polylog}(m)$. Compléter cette réduction pour tous les adversaires $\mathcal{A}^\ell_{m\mathsf{BC_H}}$ non triviaux.	50
P6.	$\mathcal{A}^1_{m\mathsf{BC_H}} \leq_\exists \mathcal{A}_{n\mathsf{QMC}}$	Soit $m = 2n$. Compléter cette réduction pour tous les adversaires $\mathcal{A}_{n\mathsf{QMC}}$ non triviaux.	50
P7.	$\mathcal{A}^\ell_{m\mathsf{BC_H}} \leq_\exists \mathcal{A}_{n\mathsf{QMC}}$	Soient $m = 2n$, $\ell \in \mathrm{polylog}(n)$. Compléter cette réduction pour tous les adversaires $\mathcal{A}_{n\mathsf{QMC}}$ non triviaux.	40

Fig. 6.1 – *Problèmes non résolus et avenues de recherche*

	Sujet	Problème	Cote
P8.	$\mathcal{A}_{n\mathsf{QMC}} \leq_{\exists} \mathcal{A}_{\mathsf{OT_S}}$	Donner les détails de cette réduction.	40
P9.	$\leq_{\exists}$	Les réductions non uniformes peuvent-elles être “uniformisées” d'une façon simple?	50
P10.	$\mathcal{A}_{n\mathsf{QMC}}$	Définir clairement ce qu'est un adversaire non trivial.	40
P11.	QMC	La mise en gage de mesure comme primitive cryptographique: y a-t-il d'autres applications que le transfert inconscient?	50
P12.	QMC	La mise en gage de mesure se généralise-t-elle utilement à d'autres mesures sur d'autres états?	50
P13.	QOWP	Qu'est-ce qu'un bon candidat au titre de permutation à sens unique quantique?	?

Fig. 6.2 – *Problèmes non résolus et avenues de recherche (suite)*

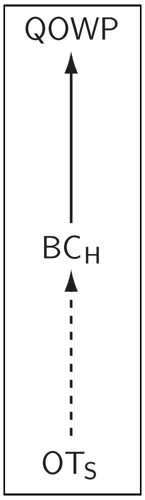


Fig. 6.3 – *Hiérarchie des primitives étudiées dans cette thèse*

Nous démarrons avec la figure 6.3[126] qui est un détail de la figure 1.3[14], une hiérarchie de primitives cryptographiques dans le monde quantique. La figure 6.3[126] ne montre que les primitives que nous avons étudiées dans cette thèse. Rappelons qu'une flèche de P_1 à P_2 désigne une réduction $P_1 \leq P_2$, c'est-à-dire qu'on réalise la primitive P_1 étant donnée la primitive P_2. Une flèche pointillée montre que la sécurité associée à P_1 n'a été que partiellement démontrée pour cette réduction. Autant que possible, nous disposons les flèches du bas vers le haut. De cette façon, les primitives apparaissant plus haut dans le diagramme sont celles qui sont *plus fortes* — dans une réduction $P_1 \leq P_2$, P_2 est intuitivement plus forte que P_1 parce que P_2 permet de réaliser P_1.

La réduction $\mathsf{BC_H} \leq \mathsf{QOWP}$ est illustrée à la figure 3.5[55] et le chapitre 3 y est entièrement dévoué. La primitive réalisée est $\mathsf{BC_H}$, la mise en gage inconditionnellement camouflante et calculatoirement liante. En effet, le théorème 3.10[57] montre que la réduction donne lieu à une mise en gage *parfaitement* camouflante.

D'autre part, la réduction $\mathsf{OT_S} \leq \mathsf{BC_H}$ est représentée à la figure 5.1[80], il s'agit du protocole de transfert inconscient auquel nous avons consacré le chapitre 5. Le sigle OT_S signifie que le bit de choix de la réceptrice Alice est inconditionnellement camouflé à Bob et le transfert camoufle calculatoirement un des deux bits a_0 ou a_1 à Alice. Le fait que le bit de choix soit inconditionnellement caché est discuté à la section 5.2[83].

Chacune de ces deux réductions comporte un côté calculatoire, et selon le paradigme que nous avons introduit à la section 1.3.2[9], on montre la sécurité calculatoire de $P_1 \leq P_2$ en exhibant une réduction $\mathcal{A}_{P_2} \leq \mathcal{A}_{P_1}$ ou $\mathcal{A}_{P_2} \leq_\exists \mathcal{A}_{P_1}$, c'est-à-dire une réduction d'un adversaire à P_2 à un adversaire à P_1, voir la figure 6.4[128]. L'adversaire $\mathcal{A}_{P_2}$ trouvé devra préserver le mieux possible les qualités de $\mathcal{A}_{P_1}$: temps de calcul polynômial et probabilité de succès non négligeable.

La réduction $\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}_{\mathsf{BC}_\mathsf{H}}$ illustrée aux figures 3.6[59], 3.7[60] et 3.8[64] ne laisse que peu de place à l'imagination. En effet, le théorème 3.19[66] montre que la probabilité de succès de l'inverseur $\mathcal{A}_{\mathsf{QOWP}}$ est au pire dans l'ordre du carré de la probabilité de succès de l'attaque à BC_H donnée, pour un coût très raisonnable en temps de calcul. Un tel résultat est difficilement perfectible. A priori, on peut espérer trouver une réduction plus sophistiquée qui donne lieu à un perte linéaire en probabilité de succès, quitte à en payer le prix en temps de calcul, mais l'intérêt d'une telle avenue de recherche est mitigé, pour ne pas dire nul.

Par contre, il serait intéressant de voir comment la réduction $\mathsf{BC}_\mathsf{H} \leq \mathsf{QOWP}$ peut se généraliser si une hypothèse moins forte que l'existence de permutations à sens unique est adoptée (P1[124]). Comment la réduction s'adapte-t-elle aux fonctions à sens unique qui ne sont pas des permutations mais des fonctions *régulières*, c'est-à-dire pour lesquelles chaque élément de l'image possède exactement un nombre fixé h de préimages? Peut-on même espérer une réduction depuis les fonctions à sens unique en général?

Une propriété du schème de mise en gage de bit du chapitre 3 est qu'il pourrait être implanté physiquement par des moyens technologiques accessibles de nos jours

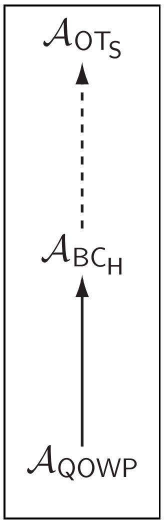


Fig. 6.4 – *Hiérarchie des adversaires*

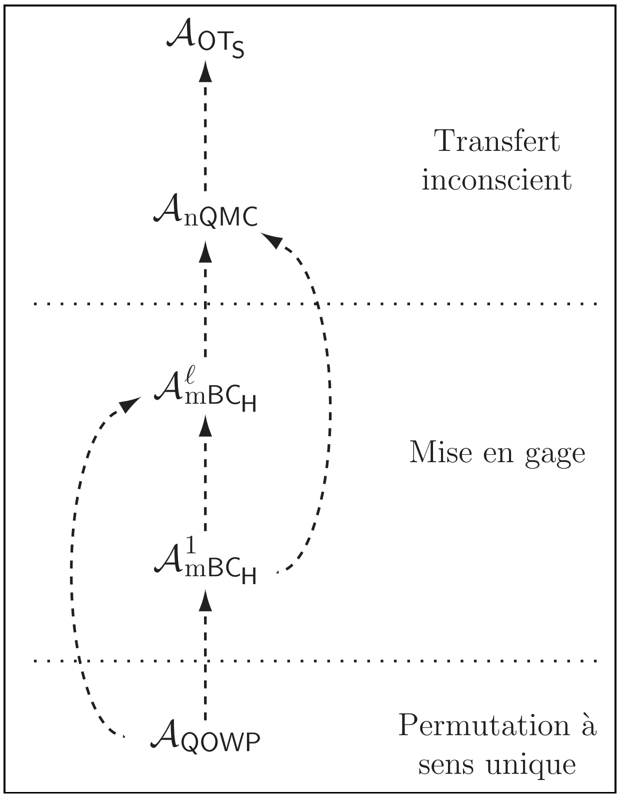


Fig. 6.5 – *Gros plan sur la hiérarchie des adversaires*

[DMS00]. Dans une telle perspective, il serait opportun de considérer un modèle de communication quantique avec possibilité d'erreurs de transmission. Comment la sécurité du schème proposé en serait-elle perturbée? Quelles dispositions devraient être mises en oeuvre afin d'implanter une primitive sécuritaire (P2[124])?

La réduction $\mathcal{A}_{\mathsf{BC_H}} \leq_\exists \mathcal{A}_{\mathsf{OT_S}}$, indiquée en pointillés à la figure 6.4[128], a été l'objet d'une suite de lemmes et de théorèmes aux chapitres 4 et 5. Afin de clarifier l'état de l'art, nous appliquons une lentille grossissante à la figure 6.4[128] pour voir apparaître la figure 6.5[128]. Nous avons regroupé les différents modèles considérés suivant trois *zones* correspondant grosso modo aux trois adversaires de la figure 6.4[128]. Nous procédons du bas vers le haut.

$\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}^1_{m\mathsf{BC_H}}$: Le modèle $\mathcal{A}^1_{m\mathsf{BC_H}}$ est techniquement différent de $\mathcal{A}_{\mathsf{BC_H}}$. L'adversaire $\mathcal{A}^1_{m\mathsf{BC_H}}$ réalise une attaque sur un *prédicat* d'une chaîne de m bits, alors que $\mathcal{A}_{\mathsf{BC_H}}$ attaque simplement la valeur d'un bit. En principe, le travail du chapitre 3 devrait être refait pour ce modèle différent. Une telle tâche ne serait toutefois pas ardue (P3[124]).

$\mathcal{A}_{\mathsf{QOWP}} \leq \mathcal{A}^\ell_{m\mathsf{BC_H}}$: Ici, le terrain est plus glissant (P4[124]). On ne voit pas immédiatement comment, par exemple, une transformation U généralisée, qui transforme des mises en gage malhonnêtes sur des chaînes de bits les unes dans les autres, pourrait être utilisée dans un inverseur comme celui de la figure 3.8[64].

$\mathcal{A}^1_{m\mathsf{BC_H}} \leq_\exists \mathcal{A}^\ell_{m\mathsf{BC_H}}$: La proposition 4.4[75], qui est facile à montrer, nous donne $\mathcal{A}_{\mathsf{BC_H}} \leq_\exists \mathcal{A}_{m\mathsf{BC_H}}$ — c'est-à-dire $\ell = m$ et m est constant par rapport au paramètre de sécurité k — mais seulement pour les adversaires $\mathcal{A}_{m\mathsf{BC_H}}$ qui sont $2^{m-1} - 1 + \epsilon(k)$-bons. Par exemple, si $m = 2$, la proposition ne concerne que les adversaires $1+\epsilon(k)$-bons, alors que l'intuition souhaiterait une réduction pour tous les adversaires $\epsilon(k)$-bons dès que $\epsilon(k) \notin \mathrm{negl}(k)$. Il s'agit d'une pierre d'achoppement sur laquelle l'auteur a buté à plusieurs reprises au cours du travail qui a mené à cette thèse. Ce n'est qu'en adoptant certaines restrictions sur l'adversaire considéré que nous avons pu établir la réduction, comme cela a été mentionné à la fin de la section 4.1[71]. Nous en faisons donc une avenue de recherche (P5[124]). Remarquons qu'en cryptographie classique, ce problème ne se présente pas. Aussitôt qu'un adversaire $\mathcal{A}^{\ell}_{m\mathsf{BC_H}}$ est $\epsilon(k)$-bon pour $\epsilon(k) \notin \text{negl}(k)$ et $\ell \in \text{polylog}(m)$, alors on peut facilement montrer qu'il existe une position, parmi m, attaquable classiquement, c'est-à-dire au sens de la définition 2.28[37] et de la ligne (2.11[37]). Les problèmes de la cryptographie quantique commencent avec la nécessité d'utiliser la ligne (2.13[38]) comme définition de la probabilité de succès d'un adversaire à la condition liante d'une mise en gage. Ensuite, les adversaires quantiques $\mathcal{A}^{\ell}_{m\mathsf{BC_H}}$ à considérer peuvent a priori créer des corrélations quantiques entre des registres qui contiennent des mises en gage sur différents bits. C'est dans ces cas que la réduction classique ne peut être transposée aveuglément au modèle quantique.

$\mathcal{A}^{1}_{m\mathsf{BC_H}} \leq_{\exists} \mathcal{A}_{n\mathsf{QMC}}$: Cette réduction-là est l'objet du théorème 5.14[107] dans le cas où $\mathcal{A}_{n\mathsf{QMC}}$ est parfait, avec $m = 2n$. Si l'extracteur est imparfait, nous devons nous contenter d'une réduction depuis $\mathcal{A}^{\ell}_{2n\mathsf{BC_H}}$ où $\ell \in \text{polylog}(n)$, voir le théorème 5.17[114]. Peut-on espérer une réduction depuis $\mathcal{A}^{1}_{2n\mathsf{BC_H}}$ même si l'extracteur est imparfait (P6[124])?

$\mathcal{A}^{\ell}_{m\mathsf{BC_H}} \leq_{\exists} \mathcal{A}_{n\mathsf{QMC}}$: Le théorème 5.17[114] montre cette réduction pour tous les extracteurs imparfaits offrant un biais non négligeable vers le bit de parité désiré, mais seulement si l'ouverture est parfaite. Le cas de l'ouverture imparfaite est discuté brièvement à la section 5.3.2.3[116]. Les détails de cette analyse restent à être explicités (P7[124]).

$\mathcal{A}_{n\mathsf{QMC}} \leq_{\exists} \mathcal{A}_{\mathsf{OT_S}}$: La section 5.3.3[117] est consacrée à cette réduction, mais certains détails formels ont été omis (P8[125]).

Une question incontournable demeure celle des réductions non uniformes (P9[125]). Peuvent-elles être remplacées par des réductions uniformes sans défigurer celles que nous avons déjà? L'argument combinatoire du lemme 5.11[103] peut-il être remplacé par quelque circuit efficace fournissant l'attaque cherchée? Par exemple, prenons le circuit de la figure 5.10[100]. Il montre qu'il est possible de produire *uniformément* n'importe quel état $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$. Le lemme 5.11[103] et la remarque 5.12[104] nous indiquent que certains de ces états doivent incarner une attaque à $2n\mathsf{BC}_\mathsf{H}$, mais aucune construction explicite n'est donnée pour les identifier, ce qui rend *non uniformes* les réductions carillonnées aux théorèmes 5.14[107] et 5.17[114]. Une façon de contourner cette difficulté consiste à dire que l'attaquant de la figure 5.10[100] connaît les portes $\widetilde{C}$ et E et qu'il peut, par précalcul, estimer toute propriété des états $|\psi_{\boldsymbol{\theta},\boldsymbol{b}}\rangle$ dont il a besoin. Dans [NC00, chapitre 8], on emprunte à la médecine le terme *tomographie* pour désigner ce type d'analyse. Il semble cependant difficile de cerner la difficulté calculatoire de cette tâche. Nous proposons donc comme avenue de recherche de rendre uniforme, mais de façon simple, les réductions de cette thèse qui font appel à la combinatoire.

Concernant le modèle d'adversaire à la mise en gage de mesure, il est pertinent de définir clairement la notion d'*adversaire non trivial* (P10[125]). Rappelons qu'un adversaire est *trivial* s'il peut être réalisé même si la primitive considérée est supposée parfaitement sécuritaire, comme si elle était donnée dans une boîte noire inattaquable. Nous nous sommes contentés de préciser deux pôles d'adversaires triviaux aux remarques 5.2[87] et 5.9[99], mais il existe un continuum de compromis entre ces deux pôles qui définit une borne inférieure sur la qualité des adversaires à considérer dans une réduction vers ou depuis $\mathcal{A}_{n\mathsf{QMC}}$. Cette tâche est un préalable aux problèmes P6[124], P7[124] et P8[125].

Le chapitre 5 a porté pour une grande part sur ce que nous avons convenu d'appeler la *mise en gage de mesure*. Nous nous en sommes servis essentiellement comme une primitive accessoire, comme un outil de preuve. Mais la mise en gage de mesure peut-elle exister comme primitive cryptographique à part entière? Autrement dit: sert-elle à autre chose (P11[125])? Une application, ou une interprétation, consiste à en faire un modèle de *canal bruyant calculatoire*. Imaginons que Bob connaît une chaîne de n bits classiques et l'envoie à Alice à travers un canal qui efface à peu près la moitié des bits et transmet correctement les autres. Ce modèle n'est rien d'autre que l'*oblivious transfer* de Rabin [Rab81]. La mise en gage de mesure réalise un tel transfert, sauf qu'ici la ressource cryptographique du bruit n'est pas fournie par une hypothèse sur l'environnement ou sur les propriétés physiques d'un canal, mais bien par une *hypothèse calculatoire*. On peut déjà réaliser le transfert inconscient de Rabin en cryptographie classique, mais ici le contexte est quantique et donc à l'abri des attaques quantiques. De plus, il n'est pas interdit d'imaginer des généralisations à des mises en gage de mesures sur des états autres que les quatre états BB84 et dans des bases autres que rectilinéaire et diagonale (P12[125]). Les propriétés cryptographiques de ces canaux restent à être analysées. On peut penser à une théorie générale de tels *canaux bruyants calculatoires*.

Nous bouclons la boucle avec la *question des candidats* (P13[125]) que nous avons déjà abordée à la section 3.2[49]. La figure 1.3[14] montre, étant donné l'état actuel de nos connaissances, qu'en cryptographie bipartite quantique, les permutations à sens unique quantiques jouent un rôle central. Quelles sont ces permutations? On l'a mentionné, les candidats au titre de permutation à sens unique ne se bousculent pas au portillon quantique. Mais qu'est-ce qu'un bon candidat? Pourquoi considère-t-on, en cryptographie classique, que la factorisation de grands entiers est un problème difficile? Parce que ce problème résiste encore et toujours à toutes les attaques, et ce, depuis des dizaines d'années, voire des centaines d'années. La science calculatoire quantique ne jouit pas d'autant d'ancienneté: elle a à peine sa majorité. Dans cent ans, on pourra se surprendre à penser que tel problème coriace résiste encore aux efforts des concepteurs d'algorithmes quantiques. On aura alors un *bon* candidat. Quoi qu'il en soit, nous avons voulu démontrer par cette thèse que la cryptographie quantique à deux parties basée sur des hypothèses calculatoires est non seulement nécessaire mais elle est possible. Un problème difficile restera une ressource précieuse pour les cryptographes, qu'ils soient *classiques* ou *quantiques*.

Bibliographie

[AC01] Mark Adcock et Richard Cleve. « A quantum Goldreich-Levin theorem with cryptographic applications ». Communication personnelle, juillet 2001.

[Amb01] Andris Ambainis. « A New Protocol and Lower Bounds for Quantum Coin Flipping ». À paraître, Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, 2001.

[BB84] C. H. Bennett et G. Brassard. « Quantum Cryptography : Public Key Distribution and Coin Tossing ». In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, décembre 1984.

[BBB+92] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, et John Smolin. « Experimental Quantum Cryptography ». *Journal of Cryptology*, 5(1):3–28, 1992.

[BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau, et Marie-Hélène Skubiszewska. « Practical Quantum Oblivious Transfer ». In *Advances in cryptology: CRYPTO '91: Proceedings*, numéro 576 in Lecture Notes in Computer Science, pages 351–366, Berlin, août 1991. International Association for Cryptologic Research, Springer-Verlag, 1992.

[BBE92] Charles H. Bennett, Gilles Brassard, et Artur K. Ekert. « Quantum Cryptography ». *Scientific American*, 267:50–57, octobre 1992.

[BCC88] Gilles Brassard, David Chaum, et Claude Crépeau. « Minimum Disclosure Proofs of Knowledge ». *Journal of Computer and System Sciences*, 37:156–189, 1988.

[BCJL93] Gilles Brassard, Claude Crépeau, Richard Jozsa, et Denis Langlois. « A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties ». In *34th Annual Symposium on Foundations of Computer Science: Proceedings*, pages 362–371, New York, novembre 1993. IEEE Computer Society, Institute of Electrical and Electronics Engineers.

[Ber97] André Berthiaume. « *Quantum Computation* », pages 23–51. In Hemaspaandra et Selman [HS97], 1997.

[Blu82] M. Blum. « Coin flipping by telephone: a protocol for solving impossible problems ». In *24th IEEE Spring Computer Conference, COMPCON: Proceedings*, pages 133–137, 1982.

[Bra85] Gilles Brassard. « Crusade for a Better Notation ». *ACM Sigact News*, 17(1):60–64, 1985.

[Bra99] Gilles Brassard. « Notes du cours d'informatique quantique ». Département d'informatique et de recherche opérationnelle, Université de Montréal, hiver 1999.

[CDvdG87] David Chaum, Ivan B. Damgård, et Jeroen van de Graaf. « Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result ». In *Advances in cryptology: CRYPTO '87: Proceedings*, numéro 293 in Lecture Notes in Computer Science, pages 87–119, Berlin, août 1987. International Association for Cryptologic Research, Springer-Verlag.

[Cle99] Richard Cleve. « An Introduction to Quantum Complexity Theory ». `http://xxx.lanl.gov/abs/quant-ph/9906111`, juin 1999.

[CLS01] Claude Crépeau, Frédéric Légaré, et Louis Salvail. « How to Convert the Flavor of a Quantum Bit Commitment ». In *Advances in Cryptology: EUROCRYPT 2001: Proceedings*, numéro 2045 in Lecture Notes in Computer Science, pages 60–77, Berlin, mai 2001. International Association for Cryptologic Research, Springer.

[Cré94] Claude Crépeau. « Quantum Oblivious Transfer ». *Journal of Modern Optics*, 41(12):2445–2454, décembre 1994.

[Cré96] Claude Crépeau. « What is going on with Quantum Bit Commitment? ». In *Proceedings of Pragocrypt '96*, pages 193–203, Prague, 1996. Czech Technical University Publishing House.

[Cré01] Claude Crépeau. Communication personnelle, 2001.

[CS91] Claude Crépeau et Miklós Sántha. « On the Reversibility of Oblivious Transfer ». In *Advances in Cryptology: EUROCRYPT '91: Proceedings*, numéro 547 in Lecture Notes in Computer Science, pages 106–113, Berlin, avril 1991. International Association for Cryptologic Research, Springer-Verlag.

[CTDL73] Claude Cohen-Tannoudji, Bernard Diu, et Franck Laloë. *Mécanique quantique.* Numéro 16 in Collection enseignement des sciences. Hermann, éditeurs des sciences et des arts, Paris, édition revue, corrigée, et augmentée d'une bibliographie étendue, 1973.

[DH76] Whitfield Diffie et Martin E. Hellman. « New Directions in Cryptography ». *IEEE Transactions on Information Theory*, 22(6):644–654, novembre 1976.

[DMS00] Paul DUMAIS, Dominic MAYERS, et Louis SALVAIL. « Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation ». In *Advances in Cryptology: EUROCRYPT 2000: Proceedings*, numéro 1807 in Lecture Notes in Computer Science, pages 300–315, Berlin, mai 2000. International Association for Cryptologic Research, Springer.

[EGL85] S. EVEN, O. GOLDREICH, et A. LEMPEL. « A Randomized Protocol for Signing Contracts ». *Communications of the ACM*, 28:637–647, 1985.

[GGM86] Oded GOLDREICH, Shafi GOLDWASSER, et Silvio MICALI. « How to Construct Random Functions ». *Journal of the ACM*, 33(4):792–807, octobre 1986.

[GJ79] Michael R. GAREY et David S. JOHNSON. *Computers and Intractability : A Guide to the Theory of NP-Completeness.* W. H. Freeman and Company, San Francisco, 1979.

[GL89] Oded GOLDREICH et Leonid A. LEVIN. « A Hard-Core Predicate for all One-Way Functions ». In STOC 1989 [STO89], pages 25–32.

[GMR89] Shafi GOLDWASSER, Silvio MICALI, et Charles RACKOFF. « The Knowledge Complexity of Interactive Proof Systems ». *SIAM Journal on Computing*, 18(1):186–208, février 1989.

[GMW87] Oded GOLDREICH, Silvio MICALI, et Avi WIGDERSON. « How to Play Any Mental Game, or A Completeness Theorem for Protocols with Honest Majority (Extended Abstract) ». In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pages 218–229, New York, mai 1987. ACM Special Interest Group for Automata and Computability Theory, ACM Press.

[Gol98] Oded GOLDREICH. « Foundations of Cryptography: Fragments of a Book ». `http://theory.lcs.mit.edu/~oded/frag.html`, février 1998.

[HILL99] Johan HÅSTAD, Russell IMPAGLIAZZO, Leonid A. LEVIN, et Michael LUBY. « A Pseudorandom Generator from any One-way Function ». *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[Hoe63] W. HOEFFDING. « Probability inequalities for sums of bounded random variables ». *Journal of the American Statistical Association*, 58:13–30, 1963.

[HS97] Lane A. HEMASPAANDRA et Alan L. SELMAN, éditeurs. *Complexity Theory Retrospective II.* Springer-Verlag, New York, 1997.

[IL89] Russell IMPAGLIAZZO et Michael LUBY. « One-way Functions are Essential for Complexity Based Cryptography ». In *30th Annual Symposium on Foundations of Computer Science*, pages 230–235, Los Alamitos, CA, octobre 1989. IEEE Computer Society, IEEE Computer Society Press.

[IR89] Russell IMPAGLIAZZO et Steven RUDICH. « Limits on the Provable Consequences of One-Way Permutations ». In STOC 1989 [STO89], pages 44–61.

[Kah96] David KAHN. *The Code Breakers.* Scribner, New York, édition révisée, 1996.

[Kil88a] Joe KILIAN. « Founding Cryptography on Oblivious Transfer ». In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 20–31, New York, mai 1988. ACM Special Interest Group for Automata and Computability, ACM Press.

[Kil88b] Joe KILIAN. « *Primality Testing and the Power of Noisy Communication Channel* ». Thèse de doctorat, Massachusetts Institute of Technology, mai 1988.

[Knu73] Donald E. KNUTH. *The Art of Computer Programming.* Addison-Wesley, Reading, MA, deuxième édition, 1973.

[LC97] Hoi-Kwong LO et H. F. CHAU. « Is Quantum Bit Commitment Really Possible? ». *Physical Review Letters*, 78(17):3410–3413, avril 1997.

[Lub96] Michael LUBY. *Pseudorandomness and Cryptographic Applications.* Princeton Computer Science Notes. Princeton University Press, Princeton, NJ, 1996.

[May96] Dominic MAYERS. « Quantum Key Distribution and String Oblivious Transfer in Noisy Channels ». In *Advances in cryptology: CRYPTO '96: Proceedings*, numéro 1109 in Lecture Notes in Computer Science, pages 343–357, Berlin, août 1996. International Association for Cryptologic Research, Springer-Verlag.

[May97] Dominic MAYERS. « Unconditionally Secure Quantum Bit Commitment is Impossible ». *Physical Review Letters*, 78(17):3414–3417, avril 1997.

[Mer79] Ralph Charles MERKLE. *Secrecy, authentication, and public key systems.* UMI Research Press, Ann Arbor, Michigan, 1979.

[MS94] Dominic MAYERS et Louis SALVAIL. « Quantum Oblivious Transfer is Secure Against All Individual Measurements ». In *Proceedings of the workshop on Physics and Computation, PhysComp '94*, pages 69–77, Dallas, novembre 1994.

[Nao91] Moni NAOR. « Bit Commitment Using Pseudorandomness ». *Journal of Cryptology*, 4(2):151–158, 1991.

[NC00] Michael A. NIELSEN et Isaac L. CHUANG. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, United Kingdom, 2000.

[NOVY98] Moni NAOR, Rafail OSTROVSKY, Ramarathnam VENKATESAN, et Moti YUNG. « Perfect Zero-Knowledge Arguments for $\mathcal{NP}$ Using Any One-Way Permutation ». *Journal of Cryptology*, 11(2):87–108, 1998.

[OVY91] Rafail OSTROVSKY, Ramarathnam VENKATESAN, et Moti YUNG. « Fair Games Against an All-Powerful Adversary (Extended Abstract) ». In Renato CAPOCELLI, Alfredo DE SANTIS, et Ugo VACCARO, éditeurs, *Sequences II: Communication, Security, and Computer Science*, pages 418–429, New York, juin 1991. Springer-Verlag, 1993.

[Rab81] M. RABIN. « How to Exchange Secrets by Oblivious Transfer ». Rapport technique TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[Sho97] Peter W. SHOR. « Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer ». *SIAM Journal on Computing*, 26(5):1484–1509, octobre 1997.

[Sim92a] Gustavus J. SIMMONS, éditeur. *Contemporary Cryptology: the Science of Information Integrity.* IEEE Press, New York, 1992.

[Sim92b] Gustavus J. SIMMONS. « *A survey of information authentication* », pages 379–419. In [Sim92a], 1992.

[STO89] ACM Special Interest Group for Automata and Computability Theory. *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*, New York, mai 1989. ACM Press.

[vdG97] Jeroen van de GRAAF. « *Towards a Formal Definition of Security for Quantum Protocols* ». Thèse de doctorat, Université de Montréal, décembre 1997.

[Wie83] Stephen WIESNER. « Conjugate coding ». *ACM Sigact News*, 15(1):78–88, 1983.

[Yao95] Andrew Chi-Chih YAO. « Security of Quantum Protocols Against Coherent Measurements ». In *Proceedings of the Twenty-Seventh Annual ACM Symposium on the Theory of Computing*, pages 67–75, New York, mai 1995. ACM Special Interest Group for Algorithms and Computation Theory, ACM Press.

[Zhu01] Hong ZHU. « Survey of Computational Assumptions Used in Cryptography Broken by Shor's Algorithm ». Mémoire de maîtrise, School of Computer Science, Université McGill, juillet 2001.