UNIVERSITÉ DE LIMOGES

ÉCOLE DOCTORALE S2IM

FACULTÉ DES SCIENCES ET TECHNIQUES

Année : 2016 Thèse N° X

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Mathématiques et Applications

présentée et soutenue par

Zoé AMBLARD

le 5 décembre 2016

Cryptographie quantique et applications spatiales.

Thèse dirigée par François ARNAULT en collaboration avec William HALIMI et Michel MAIGNAN (Thales Alenia Space)

JURY :

Eleni DIAMANTI	Chargée de Recherche, CNRS (HDR), Telecom ParisTech	Rapporteur
Jean-Pierre TILLICH	Directeur de Recherche, Inria Rocquencourt projet SECRET	Rapporteur
François ARNAULT	Maître de Conférences, Université de Limoges (HDR)	Examinateur
Thierry BERGER	Professeur, Université de Limoges	Examinateur
Frederic GROSSHANS	Chargé de Recherche, Laboratoire Aimé Cotton	Examinateur
François LAUBIE	Professeur, Université de Limoges	Examinateur
Michel MAIGNAN	Ingénieur de Recherche, Thales Alenia Space Toulouse	Invité
William HALIMI	Ingénieur de Recherche, Thales Alenia Space Toulouse	Invité

A ma famille,

Remerciements

Je tiens à remercier mon directeur de thèse, François Arnault, pour la confiance qu'il m'a accordée en acceptant d'encadrer mes travaux. Pendant ces trois années de travail, il m'a accompagnée dans mes recherches avec bienveillance et patience. Sa rigueur et son exigence vis-à-vis de la qualité scientifique de nos travaux m'ont beaucoup appris et ont grandement participé à ma formation au futur métier de chercheur.

Je remercie également mes co-directeurs, Thierry Berger, William Halimi et Michel Maignan, ainsi que l'entreprise Thales Alenia Space pour la confiance qu'ils m'ont témoignée en participant au financement et à l'encadrement de ma thèse.

Je remercie aussi les membres de mon jury de thèse pour leur participation dans l'évaluation de mon travail et pour toutes les remarques intéressantes dont il m'ont fait part afin d'améliorer mon travail. A ce titre, je remercie en particulier mes rapporteurs, Eleni Diamanti et Jean-Pierre Tillich, pour leurs suggestions et remarques ainsi que pour le temps qu'ils ont consacré à la relecture de ce manuscrit.

Je souhaite également remercier chaleureusement mes collègues du département DMI du laboratoire XLIM pour leurs conseils et leur aide dans ma formation à l'enseignement. Monsieur Necer, mon tuteur pédagogique, m'a été d'un grand soutien dans mes responsabilités d'enseignante et la passion avec laquelle il considère son métier restera pour moi un exemple.

Finalement, je remercie ma famille et l'ensemble de mes amis doctorants pour leur soutien qui m'a été précieux durant ces trois années de thèse.

Table des matières

Liste des figures et tableaux 4

Introduction 6

Vocabulaire et notations 10

Chapitre 1 : Prérequis mathématiques et formalisme de Dirac 14

1.1 Prérequis mathématiques 15
1.1.1 Produit scalaire, norme et espace de Hilbert 15
1.1.2 Propriétés des opérateurs linéaires 16
1.1.3 Définitions autour de la norme matricielle 18
1.1.4 Transformée de Fourier Discrète et matrice de Fourier 20
1.2 Prérequis de physique quantique dans le formalisme de Dirac 21
1.2.1 Réalisme local 21
1.2.2 Espace des états quantiques et vecteurs d'états 22
1.2.3 Mesure d'un système quantique 22
1.2.3.1 Mesures de Von Neumann 22
1.2.3.2 Représentation d'un qudit dans la base canonique 23
1.2.4 Mesure avec un ditter 24
1.2.4.1 Matrices de Pauli généralisées 25
1.2.4.2 Représentation mathématique 26
1.2.4.3 Mesure dans des bases sans biais 28
1.2.4.4 Mesure d'un produit d'observables incompatibles 31
1.2.5 Intrication quantique 32

Chapitre 2 : La Distribution Quantique de Clés, les protocoles usuels et leur sécurité 35

2.1 Fonctionnement des protocoles de Distribution Quantique de Clés 36
2.1.1 Les deux classes de protocoles 36
2.1.2 Les étapes principales d'un protocole 37
2.2 Les protocoles de Distribution Quantique de Clés pour qubits 38
2.2.1 Protocoles de type Prépare-et-Mesure 39
2.2.1.1 Le protocole BB84 pour qubits 39
2.2.1.2 Une variante du protocole BB84 : le protocole Six-State . 40
2.2.2 Protocoles basés sur l'intrication quantique 40
2.2.2.1 Le protocole Ekert91 pour qubits 40
2.2.2.2 Une variante du protocole E91 : le protocole BBM92 . . . 41
2.2.3 Implémentation des protocoles de Distribution Quantique de Clés . 42
2.3 La sécurité des protocoles de Distribution Quantique de Clés 45
2.3.1 Les différentes stratégies d'un attaquant 45
2.3.1.1 Quelques définitions de sécurité 46
2.3.1.2 Les modèles d'attaques théoriques 47
2.3.1.3 Les attaques de type *Quantum Hacking* et leurs contre-mesures 48
2.4 Les inégalités de Bell et la sécurité des protocoles à intrication 51
2.4.1 Choix de bases pour les inégalités CGLMP-d 52

2.4.2 Inégalités de Bell pour deux parties . . . 53
2.4.2.1 Inégalité CHSH en dimension 2 . . . 53
2.4.2.2 Inégalité CGLMP-d en dimension d . . . 54
2.4.3 Inégalités de Bell homogènes en dimension d pour n parties . . . 55
2.4.4 Rôle des inégalités de Bell dans la sécurité théorique des protocoles basés sur l'intrication . . . 57
2.4.4.1 Attaques individuelles par clonage : . . . 58
2.5 Etat-de-l'art de la sécurité des protocoles les plus courants . . . 60
2.5.1 Résumé sur la sécurité des protocoles BB84 et BBM92 . . . 60
2.5.2 Résumé sur la sécurité du protocole E91 . . . 61

Chapitre 3 : Etude théorique des inégalités de Bell homogènes en dimension d . . . 64
3.1 Comparaison avec des inégalités préexistantes . . . 65
3.1.1 Inégalité de Ji *et al.* à trois mesures par partie . . . 65
3.1.2 Réexamination de l'inégalité de Ji *et al.* . . . 67
3.1.3 Lien avec les inégalités de Bell homogènes . . . 68
3.2 Borne supérieure sur la violation des inégalités de Bell homogènes . . . 70
3.2.1 Résultats pour $n = 2$ et $d \leqslant 10$ . . . 71

Chapitre 4 : Applications cryptographiques des inégalités de Bell homogènes . . . 73
4.1 Distribution Quantique de Clés avec des qudits . . . 74
4.1.1 Le protocole NDEB pour qudits . . . 74
4.1.1.1 Sécurité du protocole NDEB . . . 76
4.1.2 Notre protocole hdDEB pour qudits . . . 78
4.1.2.1 Sécurité du protocole hdDEB . . . 79
4.1.3 Comparaison entre NDEB et hdDEB et sécurité contre les attaques individuelles par clonage . . . 81
4.2 Partage de Secret Quantique avec des qudits . . . 82
4.2.1 Mesures accordées et quasi-accordées . . . 83
4.2.2 Réinterprétation du protocole de Partage de Secret Quantique avec des bases sans biais de Yu *et al.* . . . 86
4.2.3 Ditters paramétrés par des puissances successives . . . 86
4.3 Construction de nos nouveaux protocoles de Distribution Quantique de Clés et de Partage de Secret pour qutrits . . . 88
4.3.1 Protocole de Distribution Quantique de Clés pour $d = 3$ et $n = 2$ . . . 88
4.3.2 Protocole de Partage de Secret Quantique pour $d = 3$ et $n = 3$ . . . 91

Bibliographie . . . 97

Conclusion . . . 103

Liste des figures et tableaux

1.1 Schéma de tritter pour $d = 3$ 26
2.1 Représentation des quatre bases optimales pour CHSH-3 53
2.2 Critère de sécurité contre les attaques individuelles par clonage 60
2.3 Résumé du protocole E91 62
4.1 Valeurs de violation de l'inégalité CGLMP-d pour $d = 3, 4, 5$ 77
4.2 Résumé du protocole NDEB 77
4.3 Résumé du protocole h3DEB 79
4.4 Valeurs de violation de l'inégalité hCHSH-d pour l'état $|\psi_{\mathrm{GHZ}_2}\rangle$ en fonction du polynôme homogène T_d 81
4.5 Comparaison entre les valeurs de violation des inégalités CGLMP-d et hCHSH-d 82
4.6 Tests de sécurité pour le protocole QKDd_3n_2 90
4.7 Résumé du protocole QKDd_3n_2 91
4.8 Tests de sécurité pour le protocole QSSd_3n_3 94

Introduction

La cryptographie est une science à la frontière de deux disciplines : les mathématiques et l'informatique. Depuis l'Antiquité, elle est utilisée pour protéger les communications entre plusieurs participants disposant d'un secret en commun. Ces participants chiffrent leurs messages à l'aide d'un protocole de chiffrement, c'est-à-dire en effectuant sur ces messages une série d'étapes qui les rendra inintelligibles. Seul un individu en possession du secret, qu'on appelle la *clé secrète*, pourra les déchiffrer et accéder à l'information qu'ils contiennent.

Cependant, avant même de pouvoir chiffrer leurs messages, les participants doivent disposer d'une clé secrète commune à tous. Les protocoles d'*échange de clés* servent à générer et distribuer ces clés secrètes qui jouent un rôle crucial dans la sécurité des communications. La divulgation de ce secret commun peut en effet permettre à un adversaire d'écouter les données échangées en toute impunité. En cryptographie dite *classique*, soumise aux règles de la physique classique et non pas de la physique quantique, un problème se pose : comment établir des clés secrètes communes à tous les participants avec la certitude que personne d'autre n'en ait pris connaissance ?

Pour un faible nombre de participants soumis à des contraintes géographiques minimes, ce problème peut être résolu par une rencontre physique lors de laquelle les clés seront échangées de mains en mains, chacun ayant attesté de son identité par des procédés d'*authentification*. Cette méthode devient toutefois inenvisageable dès qu'on considère des participants soumis à des contraintes de nombre ou de distance qui les empêchent de s'échanger physiquement des clés.

La cryptographie classique actuelle propose des protocoles d'échange de clés efficaces mais dont la sécurité est conditionnelle car basée sur des problèmes algorithmiques supposés (mais non prouvés) difficiles. Cette sécurité est dite *calculatoire* car elle dépend de la puissance de calcul à la disposition d'un attaquant. La cryptographie quantique, quand à elle, propose des protocoles d'échange de clés dont la sécurité est inconditionnelle car basés sur les lois de la physique quantique.

En physique, on désigne par *système* la partie de l'univers physique analysée, en opposition avec l'*environnement* qui désigne tout ce qui est hors du système. En particulier, les systèmes soumis aux lois de la physique quantique subissent de la part de l'environnement une influence qui peut être destructrice et faire progressivement disparaître les caractéristiques quantiques du système en le rapprochant d'un système classique.

Un système quantique en dimension finie d, qu'on appelle qudit, se décrit par un vecteur dans un espace de Hilbert de dimension d. Lors d'un protocole de Distribution Quantique

de Clés, on utilise des qudits pour échanger des clés en effectuant des mesures sur ces systèmes. Mais toute interaction avec un système quantique, y compris une mesure, le modifie et efface irrémédiablement une partie de l'information qu'il contient. En particulier, chaque résultat de mesure d'un système quantique dépendra des mesures effectuées précédemment sur ce même système. Ainsi, un attaquant mesurant un système pour récupérer des informations sur la clé secrète l'altèrera et y introduira des erreurs. L'absence d'erreurs sert donc de critère de sécurité et permet de s'assurer que les systèmes quantiques transmis entre les participants n'ont pas été modifiés au préalable.

L'*intrication* est un phénomène quantique qui lie plusieurs systèmes dont les propriétés physiques possèdent alors des liens statistiques forts, les *corrélations quantiques*. Ces systèmes, même spatialement séparés, ne peuvent pas être décrits indépendamment mais uniquement en tant que système quantique global.

Certains protocoles d'échange de clés quantique utilisent des systèmes intriqués. A la fin du protocole, les participants vérifient la présence d'erreurs à l'aide d'une inégalité mathématique de la catégorie des *inégalités de Bell*. En effet, le caractère quantique des corrélations de ces systèmes provoque un dépassement des bornes de l'inégalité, ce qui est impossible pour les systèmes classiques. On peut donc quantifier ce dépassement, appelé *violation* de l'inégalité, et l'utiliser pour distinguer les systèmes quantiques intriqués des systèmes classiques. Le critère de sécurité se définit alors comme suit : en cas d'absence de violation, le caractère quantique des corrélations a été altéré par interaction avec l'environnement et il y a potentiellement eu divulgation de la clé secrète.

Toute interaction avec l'environnement, et pas uniquement l'espionnage, provoque des erreurs qu'on appelle *bruit*. Le calcul de la valeur de violation d'une inégalité permet uniquement de déterminer si il y a eu altération des corrélations quantiques ou non, mais pas de conclure sur la source de cette altération. Il est donc impossible pour les participants de distinguer le bruit provoqué par une tentative d'espionnage de celui dû au milieu dans lequel on se place.

Dans un cadre expérimental réaliste, il est impossible d'éviter toute forme de perturbation naturelle et on doit donc tolérer les erreurs dues à l'interaction avec le milieu. Toutefois, en tolérant trop d'erreurs, on laisse la possibilité à un adversaire d'effectuer une attaque sans se faire repérer. On doit donc tolérer un maximum d'erreurs tout en s'assurant que cette quantité reste en dessous du bruit provoqué par l'attaque adverse la plus efficace. La valeur de violation maximale atteinte par une inégalité de Bell étant directement liée à la quantité d'erreurs tolérées par le protocole, le choix de l'inégalité est un critère important pour la résistance au bruit du protocole.

Cette thèse comporte deux sections. D'une part, une section théorique où nous étudions les propriétés des inégalités de Bell homogènes décrites par François Arnault dans [1]. Comme ces inégalités peuvent atteindre des valeurs de violation très hautes, nous les utilisons pour construire de nouveaux protocoles de cryptographie quantique plus résistants aux bruit que les protocoles actuels. D'autre part, une section pratique dans laquelle nous étudions l'intérêt de la Distribution Quantique de Clés en tant que solution complémentaire de gestion des clés pour la protection des communications spatiales.

Dans le Chapitre 1, nous résumons l'ensemble des définitions et notations nécessaires à la bonne compréhension de cette thèse.

Dans le Chapitre 2, nous donnons une description précise du fonctionnement des protocoles de Distribution Quantique de Clés et de leur implémentation. Nous nous intéressons ensuite aux différents modèles de sécurité ainsi qu'au rôle des inégalités de Bell dans la sécurité des protocoles à intrication, en accordant une attention particulière aux inégalités de Bell homogènes introduites par François Arnault dans [1]. Nous abordons également le lien entre la résistance au bruit d'un protocole de Distribution Quantique de Clés et sa sécurité contre les attaques individuelles par clonage.

Dans le Chapitre 3, nous réalisons une étude théorique des inégalités de Bell homogènes et nous analysons les possibilités d'implémentation des mesures nécessaires au test de ces inégalités avec des appareils appelés ditters, dont une description mathématique et physique est donnée par Żukowski *et al.* dans [2]. Nous déterminons également une borne supérieure sur les violations obtenues en dimension d pour n participants.

Dans le Chapitre 4, une fois ces outils théoriques établis, nous tirons profit des hautes capacités de violation des inégalités de Bell homogènes en proposant une nouvelle famille de protocoles d'échange de clés entre deux participants en dimension d, appelée hdDEB et que nous décrivons en [3]. Grâce aux valeurs de violation élevées atteintes par les inégalités de Bell homogènes, ces protocoles ont une résistance au bruit améliorée par rapport aux protocoles existants. Nous dérivons également des protocoles de cryptographie quantique en dimension 3 pour deux puis trois participants, dits respectivement Distribution Quantique de Clés et Partage de Secret Quantique, et dont la sécurité repose sur les inégalités de Bell homogènes.

Le Chapitre 5, consacré à l'étude de l'application des protocoles de Distribution Quantique de Clé dans le contexte des communications par satellite en environnement bruité, est confidentiel et a été retiré de ce manuscrit conformément au souhait de l'entreprise Thales Alenia Space.

Vocabulaire et notations

Vocabulaire

- **Cryptographie classique/quantique :** science de la protection des communications entre plusieurs parties, basée sur des phénomènes de physique classique ou de physique quantique.
- **Chiffrer :** rendre un message inintelligible pour ceux qui ne disposent pas du secret nécessaire à son déchiffrement.
- **Clé secrète :** secret commun à plusieurs participants et qui leur permet de déchiffrer leurs communications.
- **Adversaire, attaquant :** individu mal intentionné qui peut tenter de pénétrer dans un espace sans permission (*intrusion*), de se faire passer pour un utilisateur ou une procédure autorisée pour obtenir l'accès à un système (*masquarade*) ou de récupérer la clé secrète (*eavesdropping*) pour prendre illégalement connaissance des communications des participants.
- **Authentification :** procédé par lequel les participants attestent de leur identité afin d'éviter qu'un attaquant ne se fasse passer pour l'un d'eux lors d'une attaque de type *homme du milieu*.
- **Problème algorithmique difficile :** problème basé sur un énoncé mathématique qu'un adversaire ne peut résoudre en un temps suffisamment court (quantifié en semaines/mois/années) pour constituer une menace.
- **Système quantique en dimension d, qudit :** partie de l'univers analysée soumise aux lois de la physique quantique et dont on donne une description mathématique dans un espace de Hilbert $\mathcal{H}$ en dimension d.
- **Environnement :** partie de l'univers physique qui se situe hors du système.
- **Réalisme local :** le résultat d'une expérience effectuée par un observateur à un endroit donné ne peut avoir été influencé par un autre observateur situé à une distance arbitrairement grande du premier, et est pré-existante à l'expérience.
- **Issue :** résultat d'une mesure effectuée sur un système quantique.
- **Ditter :** dispositif optique permettant de mesurer des qudits grâce à la combinaison de miroirs et de déphaseurs qui modifient la phase d'une onde en entrée.
- **Intrication :** propriété spécifique à la physique quantique qui lie plusieurs systèmes, ceux-ci ne pouvant pas être décrits comme des systèmes indépendants mais uniquement comme un système global.

- **Corrélations :** liens statistiques forts entre les propriétés des systèmes quantiques intriqués.
- **Inégalités de Bell :** inégalités mathématiques dont les bornes sont dépassées par les systèmes quantiques intriqués mais pas par les systèmes classiques.
- **Violation :** dépassement des bornes classiques d'une inégalité de Bell par un système quantique intriqué.
- **Valeur de violation :** quotient de la valeur quantique sur la borne classique d'une inégalité de Bell.
- **Bruit :** erreurs introduites dans un système quantique soit par l'action de l'environnement soit par une tentative d'attaque du protocole. Si la quantité d'erreurs est trop élevée, on ne peut jamais obtenir de violation de l'inégalité de Bell choisie et la vérification de sécurité oblige à arrêter le protocole.
- **Résistance au bruit :** capacité d'obtenir une violation de l'inégalité de Bell choisie jusqu'à une valeur de bruit donnée.
- **Protocoles Prépare-et-Mesure :** classe de protocoles dans lesquels Alice choisit un bit puis prépare un qudit dans l'état quantique en conséquence avant de le transmettre à Bob. Bob mesure ensuite cet état dans une base choisie au hasard.
- **Protocoles basés sur l'intrication :** classe de protocoles dans lesquels une source prépare des qudits dans un état intriqué puis transmet sur un canal quantique un qudit à chaque participants. Ceux-ci choisissent aléatoirement une base, l'utilisent pour mesurer leur qudit et obtiennent des issues corrélées à 100%.
- **Sécurité inconditionnelle :** un attaquant avec des moyens de calculs illimités ne peut récupérer aucune information sur le texte clair même s'il en connaît le chiffré.
- **Attaques interception-réémission :** l'attaquant Eve ne peut stocker les qudits dans une mémoire quantique. Elle déroute chaque qudit destiné à Bob et le mesure dans des bases, pas obligatoirement les mêmes que celles de Bob, avant de le transmettre à son destinataire.
- **Attaques individuelles :** l'attaquant Eve peut stocker les qudits dans une mémoire quantique mais ne peut attaquer chaque qudit qu'individuellement et avec la même stratégie pour tous. De plus, Eve doit mesurer tous les états quantiques stockés avant le début du post-traitement des données.
- **Attaques collectives :** dans ces attaques qui généralisent les attaques individuelles, l'attaquant Eve doit employer la même stratégie d'attaque pour chaque qudit mais peut effectuer ses mesures après la phase de réconciliation, voire après la fin du protocole.

Notations en dimension d

- **Base canonique :** $\mathbb{B} := \{|0\rangle, ..., |d-1\rangle\}$.
- **Un état maximalement intriqué pour n qudits, appelé *état GHZ* :**
$$|\psi_{\mathrm{GHZ}_n}\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj....j\rangle_{12...n}.$$
- **Matrice adjointe d'une matrice carrée $A \in M_d(\mathbb{C})$:** $A^\dagger := \sum_{i,j=0}^{d-1} a^*_{ji} |i\rangle \langle j|$.
- **Matrice identité :** $\mathbb{I} := \sum_{j=0}^{d-1} |j\rangle \langle j|$.
- **Matrice de Fourier :** $H := \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle \langle j|$.
- **Transformée de Fourier Discrète :** $\widehat{f}(r_1, ..., r_n) := \frac{1}{d^{\frac{n}{2}}} \sum_{s \in \mathbb{Z}_d^n} \omega^{r.s} f(s)$
pour $r = (r_1, ..., r_n) \in \mathbb{Z}_d^n$, $r.s = \sum_{i=1}^{n} r_i s_i$ et $f : \mathbb{Z}_d^n \to \{1, \omega, ..., \omega^{d-1}\}$.
- **Matrice de Fourier multidimensionnelle :** $H^{\otimes n} = \frac{1}{d^{\frac{n}{2}}} \sum_{r,s \in \mathbb{Z}_d^n} \omega^{r.s} |r\rangle \langle s|$.
- **Matrices de Pauli généralisées :** $Z := \sum_{j=0}^{d-1} \omega^j |j\rangle \langle j|$ et $X := \sum_{j=0}^{d-1} |j+1\rangle \langle j|$.
- **Déphasages d'un ditter :** $\Theta = (\theta_0, ..., \theta_{d-1})$ avec $\theta_k = \mathrm{e}^{i\phi_k}$, $\phi_k \in (\phi_0, ..., \phi_{d-1})$.
- **Matrice des déphasages Θ :** $D_\Theta := \sum_{k=0}^{d-1} \theta_k |k\rangle \langle k|$.
- **Observable mesurée par un ditter de déphasages Θ :**
$$Z_\Theta := \sum_{k=0}^{d-1} \theta_k \theta^*_{k+1} |k+1\rangle \langle k|.$$
- **Ensemble des issues d'une observable Z_Θ :** $\mathfrak{U} := \{1, \omega, ..., \omega^{d-1}\}$.
- **Inégalité de Bell homogène pour deux parties :**
$\mathrm{Re}(\frac{\tau}{d^2 \cos(\frac{\pi}{d})} E(T)) \leqslant 1$ avec T un polynôme homogène.
- **Opérateur de Bell homogène :** $Q_f := \sum_{r \in \mathbb{Z}_d^n} \widehat{f}(r) \bigotimes_{i=1}^{n} X_i^{d-1-r_i} Z^{r_i}$.

Chapitre 1 :

Prérequis mathématiques et formalisme de Dirac

Dans ce chapitre, nous introduisons l'ensemble des prérequis importants à la bonne compréhension de cette thèse en séparant d'une part les définitions mathématiques essentielles et, d'autre part, des notions propres à la physique quantique comme le formalisme de Dirac et le phénomène d'intrication.

1.1 Prérequis mathématiques

1.1.1 Produit scalaire, norme et espace de Hilbert

Définition 1 Produit scalaire hermitien d'un $\mathbb{C}$-espace vectoriel E :
Considérons un espace vectoriel E sur $\mathbb{C}$. On appelle *produit scalaire hermitien* sur le $\mathbb{C}$-espace vectoriel E une application $\langle .,. \rangle : E \times E \to \mathbb{C}$ qui satisfait les hypothèses suivantes :

— Sesquilinéarité :

$\forall x_1, x_2, y \in E$ et $\lambda_1, \lambda_2 \in \mathbb{C}$

$\langle \lambda_1 x_1 + \lambda_2 x_2, y \rangle = \lambda_1 \langle x_1, y \rangle + \lambda_2 \langle x_2, y \rangle \quad$ et $\quad \langle x, y \rangle = \overline{\langle y, x \rangle}$;

— Positivité : $\quad \forall x \in E, \langle x, x \rangle \geqslant 0$;

— Définition : $\quad \forall x \in E, \langle x, x \rangle = 0 \Rightarrow x = 0_E$.

Définition 2 Espace préhilbertien complexe, espace hermitien : Le $\mathbb{C}$-espace vectoriel E muni du produit scalaire hermitien $\langle .,. \rangle$ est appelé *espace préhilbertien complexe*. Si, de plus, l'espace E est de dimension finie, il est appelé *espace hermitien*.

Définition 3 Norme d'un $\mathbb{C}$-espace vectoriel E :
Considérons un espace vectoriel E sur $\mathbb{C}$. On appelle *norme* sur le $\mathbb{C}$-espace vectoriel E une application $\|.\| : E \to \mathbb{R}^+$ satisfaisant les hypothèses suivantes :

— Définition : $\quad \forall x \in E, \|x\| = 0 \Rightarrow x = 0_E$;

— Homogénéité : $\quad \forall (\lambda, x) \in \mathbb{C} \times E, \|\lambda x\| = |\lambda| \|x\|$;

— Inégalité triangulaire : $\quad \forall (x, y) \in E^2, \|x + y\| \leqslant \|x\| + \|y\|$.

Définition 4 Produit scalaire hermitien usuel sur $\mathbb{C}^d$ et norme associée :
Pour tout $x, y \in \mathbb{C}^d$, le produit scalaire hermitien usuel sur $\mathbb{C}^d$ est décrit par :

$$\langle x, y \rangle = \sum_{i=1}^{d} x_i \overline{y_i}.$$

Soit l'application $\|x\|$ décrite par :

$$\|x\| = \sqrt{\sum_{i=1}^{d} |x_i|^2}.$$

Etant donné un espace préhilbertien complexe E muni du produit scalaire hermitien usuel, l'application $\|x\|$ est une norme sur E appelée *norme hermitienne usuelle.*

Définition 5 Espace de Hilbert complexe : On appelle *espace de Hilbert complexe* tout espace préhilbertien complexe complet pour la norme associée au produit scalaire hermitien.

Remarque : L'espace $\mathcal{H} \equiv \mathbb{C}^d$ muni du produit scalaire hermitien usuel est un espace de Hilbert complexe.

Définition 6 Vecteur normé :
Soit $\mathcal{H} \equiv \mathbb{C}^d$ un espace de Hilbert complexe de dimension d. On dit qu'un vecteur $x \in \mathcal{H}$ est *normé* si il vérifie :

$$\|x\| = 1.$$

Définition 7 Famille orthonormée :
Soit $\mathcal{H} \equiv \mathbb{C}^d$ un espace de Hilbert complexe de dimension d. On appelle *famille orthonormée* (ou orthonormale) toute famille de vecteurs de $\mathcal{H}$, notée $(e_i)_{i\in I}$, qui vérifie :

$$\forall (i,j) \in I^2, \quad (e_i, e_j) = \delta_{ij}.$$

Remarque : Tout espace de Hilbert complexe possède des bases orthonormées constructibles d'après le procédé d'orthogonalisation de Gram-Schmidt.

1.1.2 Propriétés des opérateurs linéaires

Définition 8 Opérateur linéaire : Une fonction $f : \mathcal{H} \to \mathcal{H}$ est un *opérateur linéaire* si elle vérifie les propriétés suivantes :

$$\begin{aligned} &\forall x, y \in \mathcal{H} \quad \text{et} \quad \forall \lambda \in \mathbb{C}, \\ &f(\lambda x) = \lambda f(x) \quad \text{et} \quad f(x+y) = f(x) + f(y). \end{aligned}$$

Définition 9 Isométrie :
Soient $\mathcal{H}_1$ et $\mathcal{H}_2$ deux espaces de Hilbert de dimension d. Un opérateur linéaire entre $\mathcal{H}_1$ et $\mathcal{H}_2$ est une *isométrie* si et seulement si il préserve la norme.

Définition 10 Matrice conjuguée : Soit $A \in M_d(\mathbb{C})$ une matrice carrée.
On appelle *matrice conjuguée de A* et on note A^* la matrice $(a^*_{i,j})_{0\leq i,j\leq d-1}$ avec $a^*_{i,j}$ le conjugué complexe de $a_{i,j}$.

Définition 11 Matrice transposée : Soit $A \in M_d(\mathbb{C})$ une matrice carrée.
On appelle *matrice transposée de A* et on note A^t la matrice $(a_{j,i})_{0\leq i,j\leq d-1}$.

Définition 12 Matrice adjointe : Soit $A \in M_d(\mathbb{C})$ une matrice carrée.
On appelle *matrice adjointe de A* (ou *adjoint de A*) et on note $A^\dagger$ la matrice transconjuguée de A, c'est-à-dire la matrice $(a^*_{j,i})_{0\leq i,j\leq d-1}$.

Définition 13 Soit $A \in M_d(\mathbb{C})$ la représentation matricielle d'un opérateur linéraire. On dit que A est :

- *hermitienne* si $A^\dagger = A$;
- *normale* si $A^\dagger A = AA^\dagger$;
- *unitaire* si $A^\dagger A = AA^\dagger = \mathbb{I}$.

Définition 14 Trace d'une matrice :
Etant donné une matrice carrée $A \in M_d(\mathbb{C})$, on appelle *trace* l'application $\mathrm{Tr} : M_d(\mathbb{C}) \to \mathbb{C}$, qu'on note $\mathrm{Tr}(A)$ et qui s'écrit :

$$\mathrm{Tr}(A) = \sum_{i=1}^{d} a_{ii}.$$

Proposition 1
Pour toutes matrices $A, B \in M_d(\mathbb{C})$ et pour tout scalaire $\alpha \in \mathbb{C}$, la trace vérifie les propriétés suivantes :

- $Tr(A + B) = Tr(A) + Tr(B)$,
- $Tr(\alpha A) = \alpha\, Tr(A)$,
- $Tr(A^\dagger) = Tr(A)^*$.

Théorème 1
Théorème spectral [4]
Dans un espace de Hilbert $\mathcal{H} \equiv \mathbb{C}^d$ complexe en dimension d, un opérateur linéaire est normal si et seulement si il est diagonalisable dans une base orthonormée.

Définition 15 Valeurs propres, vecteurs propres, spectre :
Soit $A \in M_d(\mathbb{C})$ la représentation matricielle d'un opérateur linéraire. La valeur $\lambda \in \mathbb{C}$ est appelée *valeur propre* de A avec x un *vecteur propre* associé si $x \neq 0_{\mathcal{H}}$ et si $Ax = \lambda x$.

L'ensemble des valeurs propres d'un opérateur linéaire A est appellé le *spectre* de A.

Définition 16 Valeurs singulières :
Les *valeurs singulières* de A sont les racines carrées des valeurs propres de $A^\dagger A$.

Définition 17 Valeur propre dominante :
La *valeur propre dominante* de A est la plus grande valeur propre en valeur absolue de A.

Définition 18 Rayon spectral :
Le *rayon spectral* $\rho(A)$ s'écrit :

$$\rho(A) = |\lambda_{max}| \text{ avec } |\lambda_{max}| \text{ la valeur propre dominante de } A.$$

1.1.3 Définitions autour de la norme matricielle

Les définitions et propriétés de la norme matricielle présentées dans cette section seront utilisées dans le Chapitre 3 pour dériver une borne supérieure sur les inégalités de Bell homogènes pour n parties en dimension d. On précise qu'on considère ici les matrices carrées dans $M_d(\mathbb{C})$.

Définition 19 Norme matricielle [5] :
Soit l'application $\|.\| : M_d(\mathbb{C}) \to \mathbb{R}$ une norme de l'espace vectoriel $M_d(\mathbb{C})$. Alors c'est une norme matricielle si, pour toutes matrices $A, B \in M_d(\mathbb{C})$, elle vérifie $\|A \cdot B\| \leqslant \|A\|\|B\|$.

Définition 20 Norme induite (ou subordonnée) :
La *norme induite* par une norme $\|.\|$ sur un $\mathbb{C}$-espace vectoriel E est une norme matricielle qui vérifie :

$$\forall A \in M_d(\mathbb{C}) \qquad \|A\| = \sup_{x \neq 0} \frac{\|Ax\|}{\|x\|} = \sup_{\|x\|=1} \|Ax\|.$$

On l'appelle aussi *norme subordonnée* à une norme $\|.\|$ sur un $\mathbb{C}$-espace vectoriel E.

Théorème 2
(Browne 1928 [6]) *Toute norme matricielle* $\|.\|$ *vérifie :*

$$\forall A \in M_d(\mathbb{C}) \quad \rho(A) \leqslant \|A\|.$$

Démonstration
Soit λ la valeur propre dominante de A et x un vecteur propre non nul associé à λ. Soit X la matrice $(x|...|x)$. On a alors :

$$|\lambda|\|X\| = \|\lambda X\| = \|AX\| \leqslant \|A\|\|X\|$$

d'où le résultat. □

Définition 21 Norme spectrale :
La *norme spectrale* $\|.\|_S$ sur $M_d(\mathbb{C})$ vérifie :

$$\forall A \in M_d(\mathbb{C}) \quad \|A\|_S = \sqrt{\rho(A^\dagger A)}.$$

Remarque : Si la matrice A est hermitienne, alors $\|A\|_S = \rho(A)$.

Définition 22 Produit scalaire hermitien canonique sur $M_d(\mathbb{C})$:
Le produit scalaire hermitien canonique sur $M_d(\mathbb{C})$, aussi appelé *produit scalaire de Frobenius*, est l'application :

$$(A, B) \in M_d(\mathbb{C})^2 \to \langle A|\ B\rangle = \sum_{i,j=1}^{n} a_{ij}^* b_{ij} = \mathrm{Tr}(A^\dagger B) = \mathrm{Tr}(AB^\dagger).$$

Définition 23 Norme euclidienne (ou de Frobenius) [7] :
La *norme euclidienne* (ou *norme de Frobenius*) $\|A\|_F^2$ sur $M_d(\mathbb{C})$ dérive du produit scalaire hermitien sur $M_d(\mathbb{C})$ et s'écrit :

$$\|A\|_F^2 = \sum_{i,j} |a_{i,j}|^2 = \mathrm{Tr}(A^\dagger A) = \sum_{val.sing.} \sigma_i^2.$$

Proposition 2
La norme induite par les normes euclidiennes est égale à la norme spectrale :

$$\|A\|_2 = \|A\|_S.$$

Démonstration
Soient $\lambda_1, ..., \lambda_d$ les valeurs propres de $A^\dagger A$ classées par ordre décroissant. Alors on a :

$$\|A\|_2^2 = \sup_{\|x\|_2=1} \|Ax\|_2^2 = \sup_{\|x\|_2=1} \langle Ax, Ax\rangle = \sup_{\|x\|_2=1} \langle A^\dagger Ax, x\rangle = \lambda_1.$$ □

Proposition 3
Pour les matrices carrées $d \times d$, la norme spectrale et la norme de Frobenius vérifient :

$$\|A\|_S \leqslant \|A\|_F \leqslant \sqrt{d}\|A\|_S.$$

Démonstration
Soient $\lambda_1, ..., \lambda_d$ les valeurs propres de $A^\dagger A$ classées par orde décroissant. On a :

$$0 \leqslant \lambda_1 \leqslant \sum_{i=1}^{d} \lambda_i \leqslant d\lambda_1.$$

En passant aux racines carrées, on obtient le résultat recherché. □

1.1.4 Transformée de Fourier Discrète et matrice de Fourier

Définition 24 Transformée de Fourier Discrète multidimensionnelle :
Soit f une application de $\mathbb{Z}_d^n$ vers $\mathfrak{U} = \{1, \omega, ..., \omega^{d-1}\}$.

La Transformée de Fourier Discrète multidimensionnelle de f est l'application $\widehat{f}(r)$ de $\mathbb{Z}_d^n$ vers $\mathfrak{U}$ définie par :

$$\widehat{f}(r_1, ..., r_n) = \frac{1}{d^{\frac{n}{2}}} \sum_{s_1,...,s_n \in \mathbb{Z}^d} \omega^{r_1 s_1 + ... + r_n s_n} f(s_1, ..., s_n) = \frac{1}{d^{\frac{n}{2}}} \sum_{s \in \mathbb{Z}_d^n} \omega^{r.s} f(s) \quad \text{pour } r.s = \sum_{i=1}^{n} r_i s_i. \tag{1.1}$$

Notons H la matrice de Fourier $H := \frac{1}{\sqrt{d}}(\omega^{ij})_{0 \leq i,j \leq d-1}$ en dimension d et $H^{\otimes n}$ la matrice de Fourier multidimensionnelle $H^{\otimes n} := \frac{1}{d^{\frac{n}{2}}}(\omega^{r.s})_{r,s \in \mathbb{Z}_d^n}$. On a donc :

$$\begin{pmatrix} \widehat{f}(0, ..., 0, 0) \\ \widehat{f}(0, ..., 0, 1) \\ .. \\ \widehat{f}(d-1, ..., d-1, d-1) \end{pmatrix} = H^{\otimes n} \begin{pmatrix} f(0, ..., 0, 0) \\ f(0, ..., 0, 1) \\ .. \\ f(d-1, ..., d-1, d-1) \end{pmatrix}$$

Lorsque $n = 2$, on obtient le cas particulier des *matrices de Hadamard*.

Cette Transformée de Fourier Discrète vérifie le théorème de Parseval énoncé ci-dessous, que nous utiliserons au Chapitre 3 pour calculer une borne supérieure sur la violation atteinte par les inégalités de Bell homogènes.

Théorème 3
Théorème de Parseval en dimension d pour n parties :
Soit f une application de $\mathbb{Z}_d^n$ vers $\mathfrak{U} = \{1, \omega, ..., \omega^{d-1}\}$ et soit $\widehat{f}(r) = \sum_{s \in \mathbb{Z}_d^n} \omega^{r.s} f(s)$ sa transformée de Fourier discrète en dimension d pour n parties.

Alors $\widehat{f}$ et f vérifient l'égalité suivante :

$$\sum_{r \in \mathbb{Z}_d^n} |\widehat{f}(r)|^2 = \sum_{r \in \mathbb{Z}_d^n} |f(r)|^2. \tag{1.2}$$

Remarque : L'égalité de Parseval montre que la Transformée de Fourier Discrète est une isométrie pour la norme euclidienne car elle vérifie $\widehat{\|f\|}_F^2 = \|f\|_F^2$.

1.2 Prérequis de physique quantique dans le formalisme de Dirac

Les progrès dans la fabrication et manipulation de particules élémentaires comme les photons ont permis de tester expérimentalement des phénomènes quantiques comme l'intrication. Ces particules sont utilisées dans des protocoles de cryptographie quantique pour transporter l'information ou établir une clé secrète partagée entre plusieurs participants. Il existe également des techniques produisant des qudits à partir d'autres particules élémentaires que les photons, comme la technique du moment cinétique orbital (OAM) avec des électrons.

En dimension d pour $d \geqslant 2$, on a différentes manières d'encoder de l'information sur un photon pour produire des qudits. Ainsi, on peut choisir d'utiliser des qudits intriqués encodés suivant l'angle de polarisation de plusieurs photons, ou d'utiliser différents degrés de liberté du même photon. Par exemple, une technique encode l'information sur le photon en exploitant différentes fréquences tandis qu'une autre technique consiste à envoyer un photon à travers un interféromètre par d chemins distincts de telle sorte qu'en empruntant un chemin, le photon sera détecté à l'arrivée avec un décalage temporel déterminé.

Une fois le qudit produit et éventuellement transmis à un destinataire, on obtient un résultat dit *issue* en effectuant une *mesure* sur ce qudit. Dans cette section, nous considérons les mesures dites *de von Neumann* et nous rappelons que chacune de ces mesures effectuées sur un système quantique le modifie et détermine donc les issues de la prochaine mesure.

1.2.1 Réalisme local

Définition 25 Réalisme : Le résultat obtenu lors d'une expérience est pré-existant à

celle-ci, qui ne fait que le révéler.

Définition 26 Localité : Un système n'est soumis qu'à l'influence de son environnement proche.

En physique quantique, lorsqu'un observateur effectue une mesure sur un système, son résultat est probabiliste et peut avoir été influencé par la mesure d'un autre observateur distant, ce qui contredit le principe du *réalisme local* de la physique classique. En particulier, le phénomène d'intrication et les expériences de violation d'inégalités de Bell que nous expliquerons plus loin prouvent une incompatibilité entre la physique quantique et le réalisme local.

1.2.2 Espace des états quantiques et vecteurs d'états

Le formalisme de Dirac est utilisé pour représenter mathématiquement les phénomènes quantiques. Dans ce formalisme, tout état quantique peut être décrit par un *vecteur d'état* dans un espace de Hilbert complexe de dimension d muni du produit scalaire hermitien canonique, noté $\mathcal{H} \equiv \mathbb{C}^d$.

Définition 27 Etat pur, état mixte : Un état représentable par un vecteur d'état dans un espace de Hilbert complexe $\mathcal{H}$ est appelé *état pur*. On appelle *état mixte* une combinaison statistique de différents états purs de $\mathcal{H}$.

Définition 28 Bra, ket : Un vecteur d'état dans $\mathcal{H}$ est noté $|\psi\rangle$ et appelé *ket*. Son vecteur dual dans $\mathcal{H}^*$ se note $\langle\psi|$ et est appelé *bra*.

Remarque : Tout vecteur d'état appartenant à l'espace $\mathcal{H}$ peut se décomposer dans une base $\{|\phi_i\rangle\}_{i=1,..,d}$, qu'on choisit généralement orthonormée.
Posons le ket $|\alpha\rangle = \sum_{i=1}^{d} a_i |\phi_i\rangle$ pour $a_i \in \mathbb{C}$. Le bra $\langle\alpha|$ s'écrit alors $\langle\alpha| = \sum_{i=1}^{d} a_i^* |\phi_i\rangle$.

1.2.3 Mesure d'un système quantique

1.2.3.1 Mesures de von Neumann

Dans cette thèse, on s'intéresse aux mesures appelées *mesures de von Neumann* (ou *mesures fortes*).

Le formalisme de la physique quantique s'effectuant dans un espace de Hilbert $\mathcal{H} \equiv \mathbb{C}^d$ complexe en dimension d, les mesures de grandeurs physiques et les évolutions d'un système quantique sont associées à des opérateurs appelés *observables*.

Définition 29 Observable :
Dans le formalisme de la physique quantique, toute quantité physique que l'on souhaite mesurer correspond à un opérateur linéaire sur $\mathcal{H}$ de représentation matricielle A, avec A une matrice normale telle qu'on peut toujours trouver une base orthonormée de $\mathcal{H}$ formée des vecteur propres de A. Un tel opérateur est appelé *observable*.

Définition 30 Observables non commutatives, incompatibles :
Deux observables commutent si et seulement si il existe au moins une base constituée de leurs vecteurs propres communs (qu'on appelle *base propre simultanée*). Des observables non commutatives sont dits *incompatibles* et ne peuvent être mesurés simultanément.

Lorsqu'on effectue une mesure de von Neumann, on ne peut obtenir qu'une issue correspondant à l'une des valeurs propres de l'observable qui lui est associée. De plus, effectuer cette mesure perturbe irrémédiablement le système quantique mesuré.

Effet d'une mesure de von Neumann :

Considérons la mesure associée à l'observable de représentation matricielle A. Soit $|\psi\rangle$ un état dans $\mathcal{H}$ et $\{a_k, |x_k\rangle\}$ le spectre de A.

Une mesure de A projette l'état $|\psi\rangle$ sur le vecteur propre $|x_k\rangle$ correspondant à la mesure. Les valeurs propres a_k de A correspondent alors aux différentes issues de mesure possibles, chacune pouvant être obtenue aléatoirement avec une certaine probabilité $P(a_k) = |\langle a_k|\ \psi\rangle|^2$.

Ainsi, si on mesure $|\psi\rangle$ suivant A et qu'on obtient a_k, l'état $|\psi\rangle$ est projeté sur le vecteur propre $|x_k\rangle$. Si on refait cette mesure sur le même état $|\psi\rangle$ sans que celui-ci ait évolué entre-temps, nous trouverons alors forcément a_k.

Définition 31 Valeur moyenne d'une série de mesures :
Si on effectue un grand nombre de mesures suivant la même observable de matrice A sur des systèmes quantiques identiques préparés dans le même état $|\psi\rangle$, on peut calculer la valeur moyenne :

$$E(A) = \sum_k a_k P(a_k) = \frac{\langle\psi|\, A\, |\psi\rangle}{\langle\psi|\ \psi\rangle}.$$

1.2.3.2 Représentation d'un qudit dans la base canonique

Dans cette thèse, on représente les états de la base canonique $\mathbb{B} = \{|0\rangle, |1\rangle, ..., |d-1\rangle\}$ en dimension d par les vecteurs :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ .. \\ .. \\ .. \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ .. \\ .. \\ .. \\ 0 \end{pmatrix} \qquad ... \qquad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ .. \\ .. \\ .. \\ 1 \end{pmatrix}$$

Soit $\omega = \mathrm{e}^{\frac{2i\pi}{d}}$ une racine $d^{\text{ième}}$ de l'unité et, pour $k = 0, .., d-1$, soient $\alpha_k \in \mathbb{C}$ des coefficients complexes. L'état d'un qudit s'écrit comme une superposition des d états de la base canonique $\mathbb{B}$:

$$|\psi\rangle = \sum_{k=0}^{d-1} \alpha_k |k\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + ... + \alpha_{d-1} |d-1\rangle . \tag{1.3}$$

Une mesure de cet état suivant la base canonique $\mathbb{B}$ permet d'obtenir une des issues $1, \omega, \omega^2, ..., \omega^{d-1}$ avec les probabilités $|\alpha_0|^2, |\alpha_1|^2, ..., |\alpha_{d-1}|^2$, chaque issue ω^k étant arbitrairement associée au dit d'information k. Ainsi, un qudit correspond à une superposition des dits $0, 1, 2, ..., d-1$.

Pour $k = 0, ..., d-1$, les probabilités $|\alpha_k|^2$ associées aux issues k vérifient la *contrainte de normalisation* qui s'écrit $\sum_{k=0}^{d-1} |\alpha_k|^2 = 1$.

Remarque :

Dans la notation de Dirac, la matrice adjointe définie précédemment se note $A^\dagger := \sum_{i,j=0}^{d-1} a^*_{ji} |i\rangle \langle j|$, la matrice de Fourier se note $H := \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle \langle j|$ et la matrice de Fourier multidimensionnelle se note $H^{\otimes n} := \frac{1}{d^{\frac{n}{2}}} \sum_{r,s \in \mathbb{Z}_d^n} \omega^{r.s} |r\rangle \langle s|$.

1.2.4 Mesure avec un ditter

En physique quantique, une particule élémentaire peut être assimilée à une onde qui possède une phase. Un ditter est un dispositif optique constitué de miroirs semi-réfléchissants et de déphaseurs qui renvoie d rayons d'égale intensité en sortie lorsqu'on illumine n'importe lequel des d chemins d'entrée. Il est paramétré par un d-uplet d'angles $(\varphi_0, \varphi_1, ..., \varphi_{d-1})$ décrivant les décalages de phases, dits *déphasages*, qui sont effectués par ces déphaseurs sur l'onde en entrée.

On peut trouver une description mathématique d'un ditter par Żukowski *et al.* dans [2]. Ces appareils ont également donnés lieu à des réalisations expérimentales, comme pour les cas $d = 3, 4$ décrits par Mattle *et al.* dans [8].

1.2.4.1 Matrices de Pauli généralisées

Avant de donner une description mathématique d'un ditter, nous devons d'abord introduire un groupe de matrices dit *de Pauli* et préciser quelques-unes de leurs propriétés que nous utiliserons dans le Chapitre 3.

Soit $\mathbb{I}$ la matrice identité en dimension d. Dans le formalisme de Dirac, on appelle *groupe de Pauli* le groupe formé par ω et par les matrices de Pauli généralisées Z et X en dimension d décrites ci-dessous :

$$Z = \sum_{j=0}^{d-1} \omega^j |j\rangle \langle j| = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix} \tag{1.4}$$

$$X = \sum_{j=0}^{d-1} |j+1\rangle \langle j| = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Proposition 4
Les matrices de Pauli X et Z en dimension d vérifient les propriétés suivantes :

a) $ZX = \omega XZ$;

b) $Z^i X^j = \omega^{ij} X^i Z^j$ *pour tout* $i, j \in \mathbb{N}$;

c) $X^d = \mathbb{I}$ *et* $Z^d = \mathbb{I}$;

d) $X^\dagger X = \mathbb{I}$ *et* $Z^\dagger Z = \mathbb{I}$ *donc X et Z sont unitaires ;*

e) $X^{d-1} = X^\dagger$ *et* $Z^{d-1} = Z^\dagger$.

Proposition 5
Soit la matrice $P^r = X^{d-1-r} Z^r$. On a alors :

a) $\|P^r\|_F = \sqrt{d}$.

b) P^r *et* P^s *sont orthogonales selon la norme de Frobenius si* $r \not\equiv s \pmod{d}$.

c) P^r *et* $(P^s)^\dagger$ *sont orthogonales.*

Démonstration

a) La matrice P^r a exactement d coefficients non nuls, tous de module égal à 1.

b) Quand $r \not\equiv s \pmod{d}$, les matrices P^r et P^s sont à supports disjoints. Elles vérifient alors $\mathrm{Tr}((P^r)^\dagger P^s) = 0$.

c) On a toujours $\mathrm{Tr}(P^r P^s) = \omega^{-r(1+s)}\mathrm{Tr}(P^{r+s}) = 0$.

1.2.4.2 Représentation mathématique

On va maintenant préciser la description mathématique d'un ditter en dimension d en se basant sur la description de Żukowski *et al.* dans [2]. Pour $j = 0, 1, ..., d-1$, nous simplifions nos notations en posant $\Theta = (\theta_0, ..., \theta_{d-1})$ avec $\theta_j = \mathrm{e}^{i\varphi_j}$.

Un ditter paramétré par les déphasages Θ effectue sur un qudit la transformation unitaire suivante :

$$U_\Theta := HD_\Theta = \frac{1}{\sqrt{d}} \sum_{k,l=0}^{d-1} \omega^{kl}\theta_l \left|k\right\rangle \left\langle l\right|$$

où les matrices H (matrice de Fourier) et D_Θ s'écrivent respectivement :

$$H = \frac{1}{\sqrt{d}} \sum_{k,j=0}^{d-1} \omega^{kj} \left|k\right\rangle \left\langle j\right| \quad \text{et} \quad D_\Theta = \sum_{k=0}^{d-1} \theta_k \left|k\right\rangle \left\langle k\right|.$$

Exemple 1 Schéma de tritter pour $d = 3$ décrit par Greenberger *et al* dans [9]

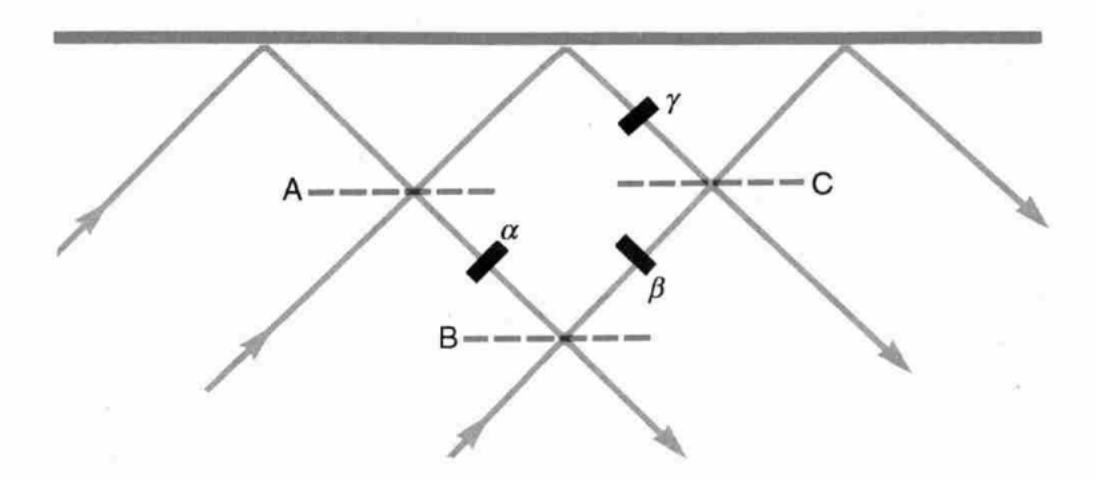


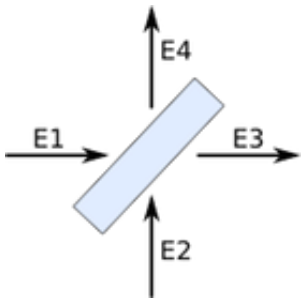
Figure 1.1 – Schéma de tritter pour $d = 3$

Un tritter peut se construire à partir de trois miroirs semi-réfléchissants, ici notés A, B, C, et de trois déphaseurs d'angles α, β, γ. En choisissant bien le coefficient de réflexion des

miroirs et les angles des déphaseurs, on peut obtenir un dispositif qui renvoie trois rayons d'égale intensité en sortie lorsqu'on illumine n'importe lequel des trois chemins d'entrée.

Représentation matricielle d'un miroir semi-réfléchissant :

Un miroir semi-réfléchissant est un miroir qui sépare un rayon d'entrée en deux flux : l'un réfléchi et l'autre réfracté, en fonction de ses coefficients de transmission et de réflexion.



On peut décrire un tel miroir par une matrice de la forme :

$$\begin{pmatrix} E_3 \\ E_4 \end{pmatrix} = \begin{pmatrix} t & r \\ r & t \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}$$

avec $T = |t|^2$ et $R = |r|^2$ les coefficients de transmission et de réflexion, qui vérifient la relation $T + R = 1$.

Le tritter décrit plus haut est constitué de trois miroirs semi-réfléchissants A, B et C, définis par leur coefficients de transmission et de réflexion respectifs $(\frac{1}{2}, \frac{1}{2})$, $(\frac{2}{3}, \frac{1}{3})$ et $(\frac{1}{2}, \frac{1}{2})$.

Les miroirs semi-réfléchissants A et C de coefficients de transmission et de réflexion $(\frac{1}{2}, \frac{1}{2})$ sont chacun décrits par la même matrice :

$$\begin{pmatrix} E_3 \\ E_4 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}$$

Le miroir semi-réfléchissant B de coefficients de transmission et de réflexion $(\frac{2}{3}, \frac{1}{3})$ est décrit par la matrice :

$$\begin{pmatrix} E_3 \\ E_4 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{2}{3}} & i\sqrt{\frac{1}{3}} \\ i\sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}$$

Au final, pour $\omega = \mathrm{e}^{\frac{2i\pi}{3}}$, le dispositif de l'exemple 1 est décrit par la matrice suivante :

$$\begin{pmatrix} \sqrt{\frac{1}{2}} & i\sqrt{\frac{1}{2}} & 0 \\ i\sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{\frac{2}{3}} & 0 & i\sqrt{\frac{1}{3}} \\ 0 & 1 & 0 \\ i\sqrt{\frac{1}{3}} & 0 & \sqrt{\frac{2}{3}} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\frac{1}{2}} & i\sqrt{\frac{1}{2}} \\ 0 & i\sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \omega & -i\omega^2 \\ i & i\omega^2 & \omega \\ i & i & 1 \end{pmatrix}$$

De plus, on obtient la matrice de Fourier tridimensionnelle $H := \frac{1}{\sqrt{3}}(\omega^{ij})_{i,j=0,..,2}$ en appliquant les déphasages suivants :

$$H = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & -i \end{pmatrix} \begin{pmatrix} 1 & \omega & -i\omega^2 \\ i & i\omega^2 & \omega \\ i & i & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & i\omega \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

Le tritter pris en exemple est bien de la forme HD_Θ avec $\Theta = (1, 1, 1)$. On peut effectuer des mesures suivant des ditters paramétrés par d'autres triplets de phase, ce qui revient dans notre exemple à ajouter des déphasages sur chacun des chemins d'entrée.

Mesure totale d'un ditter et des détecteurs :

Après avoir réalisé une telle mesure à l'aide d'un ditter, on effectue une seconde mesure dans la base canonique $\mathbb{B}$ grâce à d détecteurs de particules. Ces détecteurs mesurent l'observable de Pauli Z en dimension d :

$$Z = \sum_{k=0}^{d-1} \omega^k \left|k\right\rangle \left\langle k\right|.$$

La combinaison d'un ditter et de d détecteurs mesure donc l'observable unitaire suivante :

$$Z_\Theta := D_{\Theta^*} H^\dagger Z H D_\Theta = \sum_{k=0}^{d-1} \theta_k \theta_{k+1}^* \left|k+1\right\rangle \left\langle k\right| \tag{1.5}$$

Propriété 1

Notons $m = 1, ..., d-1$ et Z_Θ, $Z_{\Theta'}$ les observables correspondant aux ditters paramétrés par le d-uplets de déphasages $\Theta = (\theta_0, \theta_1, ..., \theta_{d-1})$ et $\Theta' = (\theta_0, \omega^m\theta_1, ..., \omega^{m(d-1)}\theta_{d-1})$ respectivement. Ces observables vérifient les propriétés suivantes :

a) L'observable Z_Θ est inchangée si on multiplie toutes les phases θ_k par un même nombre complexe μ^k qui vérifie $\mu^d = 1$.

b) Les observables Z_Θ et $Z_{\Theta'}$ vérifient $Z_{\Theta'} = \omega^{-m} Z_\Theta$ et, comme on peut toujours compenser le terme ω^{-m} en multipliant l'issue de la mesure par ω^m, elles sont mesurées par le même ditter.

1.2.4.3 Mesure dans des bases sans biais

En dimension d, on appelle *bases sans biais* et on désigne par l'abréviation MUBs les d bases orthonormales introduites par Schwinger dans [10] et notées $\mathfrak{E}$ et $\mathfrak{F}$, dont les vecteur e_i et f_j vérifient, pour tous $0 \leqslant i, j \leqslant d-1$, la relation :

$$|\langle e_i, f_j \rangle| = \frac{1}{\sqrt{d}}$$

Ces bases sont dites *sans biais* ou *mutuellement non biaisées* car une mesure effectuée sur un état quantique dans l'une de ces bases n'apporte aucune information sur le résultat de la mesure du même état dans une autre base sans biais.

On peut décrire les observables correspondant aux mesures des d MUBs, pour d premier, par les matrices :

$$Z \quad \text{et} \quad XZ^j = \sum_{k=0}^{d-1} \omega^{kj} \left|k+1\right\rangle \left\langle k\right|, \quad \text{pour} \quad j = 1, ..., d. \tag{1.6}$$

L'observable Z correspond en particulier à la mesure dans la base canonique $\mathbb{B}$.

Proposition 6
Les d observables XZ^j correspondant aux mesures des d MUBs, pour d premier, sont associées aux ditters paramétrés par les déphasages :

$$\forall k = 0, ..., d-1 \quad \theta_k = \omega^{-j\frac{k(k-1)}{2}}.$$

Démonstration
Pour tout $j = 0, ..., d-1$, on a :

$$\begin{aligned} \forall k = 0, ..., d-1 \quad \theta_k \theta_{k+1}^* &= \omega^{kj} \\ \theta_{k+1} &= \theta_k \omega^{-kj}. \end{aligned}$$

On peut réécrire ce résultat en fonction de θ_0 :

$$\begin{aligned} \forall k = 0, ..., d-1 \quad \theta_k &= \theta_{k-1}\omega^{-(k-1)j} \\ &= \theta_0 \omega^{-j\sum_{u=1}^{k}(k-u)} \\ &= \theta_0 \omega^{-j\frac{k(k-1)}{2}}. \end{aligned}$$

Si on multiplie toutes les phases par le même complexe θ_0 vérifiant $|\theta_0| = 1$, on ne modifie pas l'observable mesurée par les déphasages correspondants. Tous ces déphasages définissent donc la même mesure que les déphasages suivants :

$$\forall k = 0, ..., d-1 \quad \theta_k = \omega^{-j\frac{k(k-1)}{2}}. \qquad \square$$

Remarque : Pour tout $j = 0, ..., d-1$, quand d est impair, on a $\theta_{d-1} = \omega^{-j}$.

Exemple 2 On peut calculer explicitement les cas $d = 3, 5, 7$ ci-dessous :

d	Déphasages en fonction de j
3	$(1, 1, \omega^{-j})$
5	$(1, 1, \omega^{-j}, \omega^{-2j}, \omega^{-j})$
7	$(1, 1, \omega^{-j}, \omega^{-2j}, \omega^{-6j}, \omega^{-3j}, \omega^{-j})$

En particulier, pour $d = 3$, on obtient les déphasages suivants selon les valeurs de j :

j	Observable	Déphasages
0	X	$(1, 1, 1)$
1	XZ	$(1, 1, \omega^2)$
2	XZ^2	$(1, 1, \omega)$

1.2.4.4 Mesure d'un produit d'observables incompatibles

Les inégalités de Bell homogènes que nous étudions dans cette thèse et dont une description précise est donnée dans le Chapitre 2 font intervenir des produits d'observables nécessitant des appareils de mesure spécifiques.

En effet, ayant mesuré deux quantités A_0 et A_1 en physique classique, on peut obtenir directement le produit A_0A_1 en multipliant les résultats obtenus. En revanche, en physique quantique, ces mesures sont incompatibles et on ne peut donc pas directement déterminer A_0A_1 à partir des résultats obtenus par les mesure de A_0 et A_1 car on ne peut mesurer A_0 et A_1 simultanément. On devra donc effectuer une troisième mesure pour obtenir l'issue correspondant au produit A_0A_1.

Dans cette section, nous montrons comment mesurer un produit d'observables quantiques à l'aide d'un dispositif dédié, incluant un ditter, dont nous donnons une description mathématique et physique.

Proposition 7
Soient $u = 1, .., d-2$ et $v = d-1-u$. Le produit des deux observables Z_Θ^u et Z_Λ^v s'écrit :

$$Z_\Theta^u Z_\Lambda^v = Z_\Gamma^\dagger$$

avec Z_Γ l'observable correspondant au ditter paramétré par le d-uplet

$$\Gamma = (\gamma_0, \gamma_1, ..., \gamma_{d-1}) \quad avec \quad \gamma_k = \theta_{k-u}^* \theta_{k-u+1}^* ... \theta_{k-1}^* \lambda_{k+1}^* \lambda_{k+2}^* ... \lambda_{k+v}^*. \tag{1.7}$$

Démonstration
Soient $u = 1, ..., d-2$ et $v = d-u-1$.

Dans notre description de la famille de protocoles hdDEB en [3], on écrit :

$$Z_\Theta^u Z_\Lambda^v = \sum_{k=0}^{d-1} \theta_{k-u} \theta_k^* \lambda_{k+1} \lambda_{k-u}^* \left|k\right\rangle \left\langle k+1\right|. \tag{1.8}$$

Or, pour toute mesure d'observable Z_Ω, on a $Z_\Omega^{d-1} = D_\Omega^* H^\dagger Z^\dagger H D_\Omega = Z_\Omega^\dagger$.

Pour réécrire ce produit d'observables comme une nouvelle mesure, les déphasages doivent donc vérifier :

$$\gamma_{k+1}\gamma_k^* = \theta_{k-u}\theta_k^*\lambda_{k+1}\lambda_{k-u}^*.$$

L'une des solutions possible est :

$$\forall k = 0, ..., d-1 \qquad \gamma_k = \theta_{k-u}^*\theta_{k-u+1}^*...\theta_{k-1}^*\lambda_{k+1}^*\lambda_{k+2}^*...\lambda_{k+v}^*. \qquad \square$$

D'après la description de l'observable Z_Θ en (1.5), on en conclut que n'importe quelle observable $Z_\Theta^u Z_\Lambda^v$ peut s'implémenter grâce au ditter paramétré par le d-uplet de déphasages $\Gamma = (\gamma_0, .., \gamma_{d-1})$ et aux d détecteurs effectuant une mesure correspondant à l'observable $Z^\dagger$ au lieu de Z.

1.2.5 Intrication quantique

Dans le phénomène appelé *intrication*, qui est spécifique à la physique quantique, les objects intriqués possèdent un état quantique global et ne peuvent être décrits séparément même s'ils sont situés à de grandes distances l'un de l'autre. De plus, les propriétés physiques de ces objets intriqués exhibent des corrélations élevées.

Effectuer des mesures bien choisies sur des qudits intriqués permet d'obtenir des issues aléatoires mais foretment corrélées, ce qui est très utile dans le partage d'une clé secrète.

Description mathématique de l'intrication :

L'état global de n systèmes quantiques peut être représenté de deux façons : soit comme un état *séparable*, c'est-à-dire un produit tensoriel de n qudits $|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle$ avec $|\psi_i\rangle$ l'état du système i, soit comme un état intriqué.

Définition 32 Etat intriqué : Soit $|\psi\rangle \in \mathcal{H}^k$. L'état $|\psi\rangle$ est dit *intriqué* si il ne peut être factorisé (en terme de produit tensoriel) en plusieurs états, c'est-à-dire s'il n'existe pas de $|\psi_i\rangle \in \mathcal{H}^{m_i}$ tels que $|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle$ et $k = \sum_{i=1}^{n} m_i$.

Dans ce cas, les prévisions des issues de mesure d'un des systèmes i ne peut plus s'exprimer en fonction de $|\psi_i\rangle$. On doit alors utiliser la formule de la valeur moyenne de l'observable A dans l'état $|\psi\rangle$ décrite en (31).

De plus, la mesure d'une des particules affecte instantanément l'état global du système, donc les autres particules intriquées.

Définition 33 Etat maximalement intriqué : Un état est dit *maximalement intriqué* si il y a corrélation parfaite entre les particules qui composent le système.

Définition 34 Etat GHZ : On appelle *état GHZ* l'un des états maximalement intriqués en dimension d pour n qudits, décrit par :

$$|\psi_{\mathrm{GHZ}_n}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj....j\rangle_{12...n} \,. \tag{1.9}$$

Exemple 3 : Paire de qudits intriqués

Soient deux qudits A et B intriqués dans un état maximalement intriqué :

$$|\psi_{\mathrm{GHZ}_2}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle \,. \tag{1.10}$$

Une mesure du qudit A suivant la base canonique $\mathbb{B}$ permet d'obtenir chaque issue k avec la probabilité $|\frac{1}{\sqrt{d}}|^2 = \frac{1}{d}$. Cependant, lorsqu'on effectue cette mesure sur A et qu'on obtient l'issue k, l'état $|\psi_{\mathrm{GHZ}}\rangle$ est projeté vers le nouvel état $|\psi'_{\mathrm{GHZ}}\rangle = |kk\rangle$. Une mesure de B suivant la base canonique $\mathbb{B}$ donnera alors l'issue k avec une probabilité égale à 1.

Dans la base canonique $\mathbb{B}$, mesurer A détermine donc totalement l'issue de la mesure de B et les issues obtenues seront corrélées à 100%.

Conclusion

Nous avons abordé dans l'introduction le problème de l'échange de clés en cryptographie classique et expliqué en quoi certains phénomènes quantiques, en particulier l'intrication, permettent à la cryptographie quantique de proposer des alternatives intéressantes en offrant la possibilité de détecter les perturbations d'un protocole d'échange de clés.

Dans ce chapitre, nous avons présenté la majeure partie des notions et définitions nécessaires à la bonne compréhension de cette thèse. Nous avons d'abord rappelé le contexte mathématique du formalisme de Dirac utilisé dans la physique quantique en nous plaçant dans un espace de Hibert complexe muni du produit scalaire canonique et de sa norme associée. Nous avons en particulier insisté sur de nombreuses définitions et propriétés de la norme matricielle que nous utiliserons dans le Chapitre 3 pour établir une borne supérieure sur la valeur de violation atteignable par la famille des inégalités de Bell homogènes.

Nous avons ensuite présenté le Formalisme de Dirac, ses notations usuelles et la famille des mesures de von Neumann ainsi que le vocabulaire qui leur est associés. Nous avons abordé les notions de réalisme local et d'observables normales dont les valeurs propres correspondent aux issues des mesures. Finalement, afin d'utiliser plus tard les inégalités de Bell homogènes qui atteignent des valeurs de violation très hautes, nous avons montré comment mesurer des produits d'observables avec des ditters et nous avons donné quelques précisions sur le phénomène d'intrication utilisé dans certains protocoles de Distribution Quantique de Clés.

Chapitre 2 :

La Distribution Quantique de Clés, les protocoles usuels et leur sécurité

Dans ce chapitre, nous nous intéressons aux protocoles cryptographiques permettant d'établir les clés secrètes nécessaires au chiffrement des communications entre deux parties et appelés protocoles de Distribution Quantique de Clés.

Ces protocoles, qui se regroupent en deux grandes classes selon s'ils exploitent ou non le phénomène d'intrication, se divisent en plusieurs étapes. La première consiste à échanger des états via un canal de communication quantique implémenté grâce à des appareils optiques et s'achève avec l'obtention des issues de mesure classiques. Les étapes suivantes réunissent une série de traitements réalisés sur les issues classiques tandis que les participants échangent les informations nécessaires à ces post-traitements sur un canal classique public et authentifié.

Nous commencerons par décrire chaque étape des deux grandes classes de protocoles de Distribution Quantique de Clés et les appareils utilisés pour les implémenter. Nous donnerons en particulier comme exemples des descriptions précises des protocoles pour qubits les plus couramment utilisés, en particulier les protocoles BB84, E91 et BBM92. Nous aborderons ensuite la sécurité de la Distribution Quantique de Clés en distinguant les attaques théoriques visant les protocoles des attaques pratiques portant sur l'implémentation. Nous terminerons sur un paragraphe consacré au lien entre la sécurité des protocoles dits *à intrication*, le bruit présent sur le canal quantique et le test de la violation d'une inégalité de Bell.

2.1 Fonctionnement des protocoles de Distribution Quantique de Clés

2.1.1 Les deux classes de protocoles

En Distribution Quantique de Clés, on peut faire la distinction entre deux classes de protocoles : les protocoles de type *Prépare-et-Mesure* (P & M) et les protocoles basés sur l'intrication, dits *à intrication*. Ces protocoles se différencient par le type d'états quantiques transmis (intriqués ou non), donc par la phase de préparation de ces états, ainsi que par le processus de vérification de la présence d'un attaquant. En effet, dans le cas d'un protocole à intrication, il est possible d'effectuer cette vérification au moyen d'un objet mathématique appelé *inégalité de Bell*.

Définition 35 Protocoles de type Prépare-et-Mesure :
Alice choisit un bit puis prépare un qudit dans l'état quantique en conséquence avant de le transmettre à Bob. Bob mesure ensuite cet état dans une base choisie au hasard et obtient une issue classique.

Définition 36 Protocoles à intrication :
Une source prépare une paire de qudits dans un état intriqué à deux parties puis transmet sur un canal quantique un qudit de chaque paire à Alice et l'autre à Bob. Ceux-ci choisissent aléatoirement une base parmi l'ensemble des bases à leur disposition, mesurent leur qudit dans cette base et obtiennent chacun une issue classique. Grâce à l'intrication, lorsque Alice mesure son état dans une base choisie au hasard, l'état de Bob est projeté sur l'état correspondant à la mesure d'Alice.

2.1.2 Les étapes principales d'un protocole

Un protocole de Distribution Quantique de Clés fait intervenir deux canaux : un canal quantique implémenté à l'aide d'appareils optiques sur lequel transitent les objets quantiques et un canal classique *authentifié*.

L'authentification est une étape préliminaire cruciale car elle sert à empêcher une attaque du type *homme au milieu* dans laquelle un adversaire usurpe l'identité des participants. Le canal classique authentifié peut par exemple être obtenu à partir d'un canal classique non sécurisé et d'un court secret partagé en utilisant des *codes d'authentification de messages (MACs)*. On peut choisir un code basé sur une fonction de hachage et standardisé comme HMAC, ou un code basé sur une fonction de hachage universelle comme ceux introduits par Wegman et Carter en 1979 dans [11] et en 1981 dans [12], puis développés par Stinson en 1991 dans [13].

Un tel protocole se divise généralement en plusieurs phases successives que nous détaillons plus bas : la communication quantique, la divulgation et réconciliation des bases de mesure, l'estimation et correction des erreurs, l'amplification de confidentialité.

Protocole de Distribution Quantique de Clés :

1. *Communication quantique :* Cette étape, qui diffère selon la classe du protocole considérée, fait intervenir la préparation, la transmission et la mesure des états quantiques. Elle se répète jusqu'à ce que les participants aient mesuré et collecté un nombre suffisant d'issues classiques.

2. *Réconciliation des bases :* Alice et Bob révèlent sur le canal classique authentifié les bases utilisées et trient leurs issues en conséquence. Certaines issues sont utilisées pour dériver la clé secrète, certaines pour tester la sécurité et d'autres sont simplement mises au rebut.

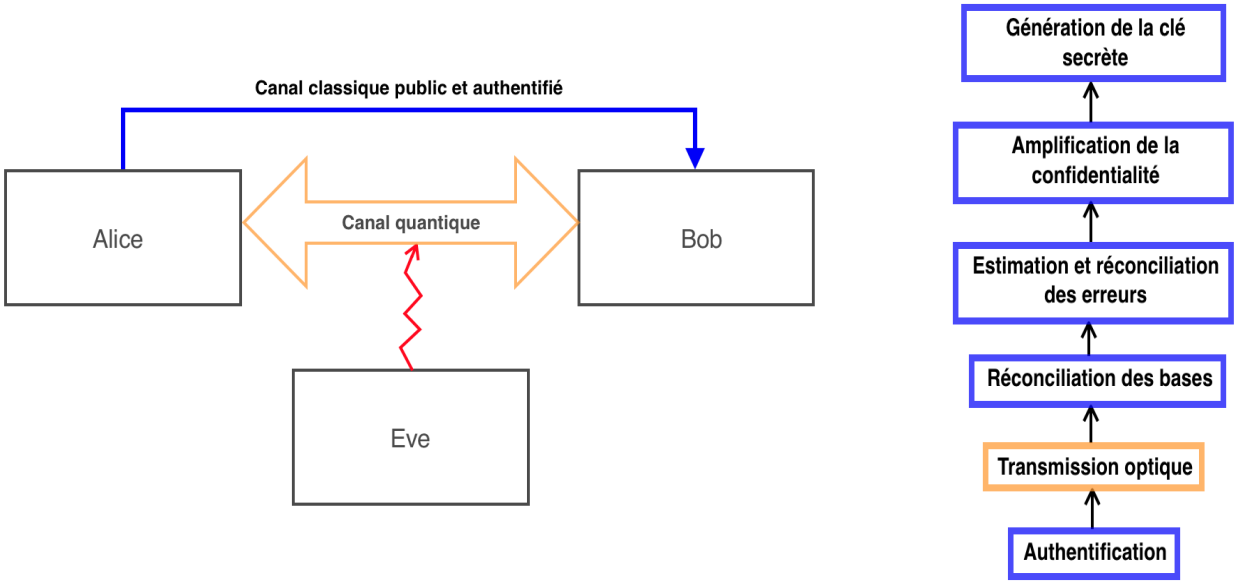
3. *Estimation du taux d'erreur :* Alice et Bob dévoilent publiquement les issues choisies lors de la phase précédente pour servir aux tests de sécurité puis les utilisent pour

estimer le taux d'erreur. Grâce à ce taux, ils évaluent la possibilité qu'un adversaire dissimule ses attaques en les faisant passer pour ces erreurs. Suivant leur conclusion, ils peuvent choisir d'arrêter là le protocole et de le recommencer si il y a un risque de compromission de la clé.

4. *Correction d'erreur :* selon le taux d'erreur estimé précédemment, Alice et Bob peuvent utiliser une procédure de correction des erreurs, par exemple un code correcteur d'erreurs quantique, pour éliminer les différences entre leurs issues.

5. *Amplification de confidentialité :* Alice et Bob obtiennent une clé secrète à partir de leurs issues partagées, par exemple en utilisant une fonction de hachage universelle.

Remarque : L'étape de communication quantique est la seule qui fait intervenir le canal quantique. Toutes les étapes de traitement des données classiques se déroulent via des échanges sur le canal classique authentifié et sont généralement regroupées sous le même terme de *post-traitement des données (post-processing)*. De plus, il est possible de stocker ces issues classiques pour réaliser ultérieurement la phase de post-traitement.



2.2 Les protocoles de Distribution Quantique de Clés pour qubits

Dans cette section, nous nous intéressons aux protocoles de Distribution Quantique de Clés utilisant des systèmes quantiques en dimension 2 appelés qubits. Nous commençons par une description du premier protocole de Distribution Quantique de Clés de type Prépare-et-Mesure pour qubits décrit par Bennett et Brassard dans [14] et appelé BB84, et sa variante décrite par Brußdans [15], le protocole Six-State. Nous présentons ensuite le

premier protocole basé sur l'intrication quantique pour qubits décrit par Ekert dans [16] et appelé Ekert91 ou E91, et sa variante décrite par Bennett *et al* dans [17], le protocole BBM92.

2.2.1 Protocoles de type Prépare-et-Mesure

2.2.1.1 Le protocole BB84 pour qubits

Le protocole BB84 en dimension 2, premier protocole de Distribution Quantique de Clés, est initialement décrit par Bennett et Brassard dans [14] et appelé BB84. Il permet à Alice de transmettre à Bob une clé secrète aléatoire en encodant les bits secrets suivant la direction de polarisation des photons.

Déroulement du protocole BB84 et bases utilisées :

Les étapes 1 et 2 permettent à Alice et Bob de collecter des issues qu'ils trient ensuite lors des étapes 3 et 4 pour obtenir une clé partagée.

Alice et Bob mesurent la direction de polarisation des photons suivant deux bases orthogonales $\{|0\rangle, |1\rangle\}$ et $\{|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, appelées respectivement base rectiligne et base diagonale. Ces bases appartiennent à la famille des bases sans biais décrites dans le Chapitre 1.

Procédure :

1. Alice choisit une suite de bits aléatoire. Pour chaque bit, elle tire au hasard l'une de ses deux bases et l'utilise pour encoder le bit concerné. Elle transmet ensuite l'état quantique correspondant à Bob.

2. Pour chaque état reçu, Bob tire au hasard l'une de ses deux bases et mesure l'état suivant cette base.

3. Alice et Bob annoncent publiquement sur un canal classique authentifié leurs choix de bases respectifs.

4. Alice et Bob ne conservent que les bits dont les choix de bases coïncident pour dériver une clé secrète commune. Les bits ne vérifiant pas cette condition sont mis au rebut.

2.2.1.2 Une variante du protocole BB84 : le protocole Six-State

Le protocole Six-State décrit par Bruß dans [15] est une variante du protocole BB84 qui utilise trois bases sans biais au lieu de deux. L'ajout de cette troisième base $\{|\circlearrowleft\rangle := \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), |\circlearrowright\rangle := \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)\}$, appelée base circulaire, simplifie l'étude de sa sécurité et réduit la probabilité que l'espion devine au hasard la base utilisée par Alice.

En revanche, les bases choisies par Alice et Bob ne coïncident plus qu'avec une probabilité $\frac{1}{3}$ au lieu de $\frac{1}{2}$, ce qui réduit le taux de génération de clés par rapport à BB84. En termes d'implémentation, l'ajout d'une base de mesure implique également l'ajout de dispositifs supplémentaires, donc de bruit dans le canal quantique.

2.2.2 Protocoles basés sur l'intrication quantique

2.2.2.1 Le protocole Ekert91 pour qubits

Le protocole Ekert91 en dimension 2, décrit par Arthur Ekert en 1991 dans [16] et abrégé en E91, permet à Alice et Bob d'exploiter les propriétés de l'intrication quantique pour partager une clé secrète aléatoire en mesurant des paires de qubits intriqués.

Grâce au phénomène d'intrication présenté dans le Chapitre 1, Alice et Bob savent que si des qubits appartenant à la même paire intriquée sont mesurés dans la même base, les issues obtenues sont corrélées à 100%. Ils peuvent donc utiliser cette propriété pour établir une clé secrète commune.

De plus, Alice et Bob peuvent déterminer si le protocole a été perturbé par un bruit environnemental ou par un espion. En effet, certaines issues non corrélées obtenues en mesurant les qubits dans des bases différentes peuvent tout de même être utilisées pour vérifier la violation d'une inégalité de Bell. En cas de violation, Alice et Bob peuvent utiliser la clé sans crainte d'avoir été écoutés.

Dans le protocole E91, chaque participant dispose de quatre bases de mesure que nous décrivons plus bas.

Remarque :

Le protocole originel ne faisait intervenir que trois bases de mesure mais, tout comme on peut passer du protocole BB84 au protocole Six-State, la prise en compte d'une base de mesure supplémentaire dans le protocole E91 permet d'assurer une meilleure sécurité sans augmenter significativement la complexité du protocole [4], au prix toutefois d'une réduction du taux de génération de clés et d'ajout de dispositifs, donc de bruit.

Déroulement du protocole E91 et bases utilisées :

Les étapes 1 et 2 permettent à Alice et Bob de collecter des issues qu'ils trient ensuite lors des étapes 3 et 4 pour obtenir une clé partagée.

Alice et Bob mesurent la direction de polarisation des photons suivant quatre bases définies pour $k, l = 0, 1, 2, 3$ par les angles $A_k = \frac{k\pi}{4}$ et $B_l = \frac{l\pi}{4}$ respectivement.

Procédure :

1. Alice et Bob reçoivent de la source des paires de qubits intriqués dans l'état $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.
2. Pour chacun de ces états, Alice tire au hasard un $a \in \{0, 1, 2, 3\}$ et effectue la mesure correspondant à la base A_a tandis que Bob fait de même pour un $b \in \{0, 1, 2, 3\}$ et mesure suivant la base B_b.
3. Alice et Bob révèlent publiquement sur un canal classique authentifié la séquence des bases utilisées pour effectuer leurs mesures.
4. Lorsque $a = b$, les résultats obtenus sont parfaitement corrélés et Alice et Bob peuvent utiliser les bits résultants pour dériver une clé secrète commune.

2.2.2.2 Une variante du protocole E91 : le protocole BBM92

Le protocole E91 a été beaucoup étudié dans le cas d'une variante pour deux bases de mesure, le protocole BBM92 décrit par Bennett *et al* dans [17]. Dans ce protocole, lorsque Alice mesure son état intriqué dans une base au hasard, l'état de Bob est projeté sur l'état correspondant à la mesure d'Alice. Cette mesure d'Alice suivie de la projection correspondante équivaut à la phase de préparation de l'état par Alice dans le protocole BB84.

Grâce à équivalence entre le protocole à intrication BBM92 et le protocole BB84 de type Prépare-et-Mesure, une preuve de sécurité obtenue pour BBM92 peut également s'appliquer, dans certaines conditions dont nous parlerons plus loin, au protocole BB84.

Déroulement du protocole BBM92 et bases utilisées :

Alice et Bob mesurent la direction de polarisation des photons suivant deux bases définies pour $k, l = 0, 2$ par les angles $A_k = \frac{k\pi}{4}$ et $B_l = \frac{l\pi}{4}$ respectivement.

Procédure :

1. Alice et Bob reçoivent de la source des paires de qubits intriqués dans l'état $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

2. Pour chacun de ces états, Alice tire au hasard un $a \in \{0, 2\}$ et effectue la mesure correspondant à la base A_a tandis que Bob fait de même pour un $b \in \{0, 2\}$ et mesure suivant la base B_b.

3. Alice et Bob révèlent publiquement sur un canal classique authentifié la séquence des bases utilisées pour effectuer leurs mesures.

4. Lorsque $a = b$, les résultats obtenus sont parfaitement corrélés et Alice et Bob peuvent utiliser les bits résultants pour dériver une clé secrète commune.

Lors des démonstrations expérimentales de protocoles pour qubits basés sur l'intrication, comme l'expérience d'Ursin *et al* dans [18], c'est souvent le protocole BBM92 qui est implémenté en tant qu'équivalent du protocole BB84 avec intrication.

2.2.3 Implémentation des protocoles de Distribution Quantique de Clés

Cette section donne un aperçu des différents appareils optiques utilisés dans l'établissement du canal quantique. Les informations présentes se basent majoritairement sur l'état-de-l'art des différents appareils implémentés et des attaques associées par Lo *et al* dans [19], ainsi que sur l'article de R. H. Hadfield dans [20] qui décrit différents types de sources, de détecteurs et leurs caractéristiques respectives.

Sources de photons :

— Les sources de type *phase-randomized weak coherent state pulses* (**WCP**) produisant des impulsions laser atténuées sont utilisées pour les protocoles de la famille Prépare-et-Mesure. En appliquant une randomisation globale sur la phase, l'état devient un mélange classique d'états de Fock (états avec des nombres de photons variables) suivant une loi de Poisson.

— Les sources de type *spontaneous parametric-down conversion* (**SPDC**) sont utilisées pour les protocoles à intrication. Un cristal non linéaire est utilisé pour diviser les faisceaux de photons en paires de photons. Leurs énergies et impulsions combinées sont égales à l'énergie et l'impulsion du photon originel à travers le cristal et leurs polarisations sont corrélées (*phase-matching*).

Détecteurs de photons uniques :

On considère plusieurs types de détecteurs variant selon les matériaux utilisés et adaptés à des longueurs d'ondes différentes. Par exemple, on peut utiliser des détecteurs basés sur des photodiodes de type SPADs (*single-photon avalanche photodiodes*) et faire varier les matériaux : Si SPAD (*silicon single-photon avalanche photodiodes*) pour des longueurs d'onde autour de 500 nm et InGaAs SPAD (InGaAs *single-photon avalanche photodiodes*) autour de 1550 nm. On peut également utiliser des détecteurs qui ne sont pas basés sur des photodiodes comme SNSPDs (*Superconducting nanowire single-photon detectors*) pour des longueurs d'onde autour de 1550 nm.

	Si SAPD	InGaAs APDs	SNSPDs
Application	air libre	fibre optique	fibre optique
Longueur d'onde λ (nm)	800	$1310, 1550$	$1310, 1550$
Sensibilité (%)	50	$50, 15$	93
Taux de *dark count*	normal	normal	élevé (100 Hz)
Taux de répétition	GHz	MHz	GHz
Température	normale	normale	basse (0.1 K)

Vocabulaire concernant les détecteurs :

— *Sensibilité :* ratio du nombre de photons détectés sur le nombre de photons émis. Lorsque cette valeur est faible, on risque d'introduire du bruit.

— *Taux de répétition :* taux de répétition maximum qu'il est possible de détecter.

— *Taux de dark count :* taux moyen de détection d'un faux signal de photon, c'est-à-dire sans lumière émise.

Résumé des paramètres usuels pour les cas air libre et fibre optique :

Dans ce qui suit, nous supposons que les objets chargés de transporter l'information quantique sont des photons. Nous distinguerons deux cas de figure dans l'implémentation des protocoles de Distribution Quantique de Clés : le transport des photons en air libre et leur transport via la fibre optique.

Implémentation des protocoles de type Prépare-et-Mesure :

	Air libre	Fibre optique
Source	WCP	WCP
Encodage (s)	polarisation	phase, time-bin, fréquence
Longueur d'onde λ (nm)	800	$1310, 1550$

Implémentation des protocoles à intrication :

	Air libre	Fibre optique
Source	SPDC	SPDC
Encodage (s)	polarisation, energy-time	energy-time
Longueur d'onde λ (nm)	800	$1310, 1550$

Technique de multiplexage dite *wavelength-division multiplexing* (WDM) :

Les expériences de Yoshino *et al* dans [21] utilisant des techniques de multiplexage comme WDM (*wavelength-division multiplexing*) ont permis de combiner deux canaux quantiques dans la *third telecom window* (longueurs d'ondes télécoms autour de 1550 nm) pour générer des taux de clés stables pendant 30 jours sans maintenance.

Ils ont obtenu un taux de clé secrète de 1 Mbps sur 35 km de fibre optique à une longueur d'onde de 1550 nm pour un signal classique avoisinant les $-18,6$ dBm. Ces techniques pourraient non seulement permettre d'accroître le taux de génération de clés, mais aussi de combiner le canal quantique avec des trafics télécoms conventionnels importants dans la même fibre optique.

Quelques remarques générales sur l'implémentation des protocoles de QKD :

— La polarisation étant plus sujette aux perturbations lors de transmission dans une fibre optique, on choisit alors généralement d'utiliser d'autres modes d'encodages.

— Le *decoy-state* est une contre-mesure contre l'attaque PNS décrite dans le paragraphe concernant la sécurité des implémentations et fréquemment implémentée en pratique. La distance maximum pour un protocole utilisant cette technique est de 150 km pour un protocole Prépare-et-Mesure et 350 km pour un protocole à intrication. Des taux de génération de clé stables ont étés obtenus pour ces deux familles de protocoles et des distances de 100 km à la fois en air libre et avec des fibres optiques.

— Pour des distances inférieures à 100km, on peut utiliser des protocoles simples à implémenter comme les protocoles de la famille *distributed-phase-reference* dont *differential-phase-shift* (DPS) ou *coherent-one-way* (COW) qui utilisent des sources WCP.

— La distance maximum peut être augmentée à 350 km en utilisant des protocoles à intrication qui supportent des pertes plus grandes (jusqu'à 70 dB) que les protocoles de la famille Prépare-et-Mesure. Dans ce cas, l'implémentation est plus compliquée et le taux de génération de clé secrète est bien plus bas.

— Dans les protocoles à intrication la source peut être placée chez l'un des participants ou entre les participants, ce qui donne lieu à des scénarios différents. Le protocole le plus fréquemment implémenté est BBM92 dans lequel la source est placée chez Alice.

2.3 La sécurité des protocoles de Distribution Quantique de Clés

L'étude de la sécurité des protocoles de Distribution Quantique de Clés est une tâche rendue difficile par le nombre de modèles différents à prendre en compte : protocole, type d'attaque ou appareils utilisés pour l'implémentation. Etant donné qu'une attaque est censée provoquer des erreurs donc du bruit, on utilise usuellement comme marqueur de la présence d'un attaquant la quantité de d'erreurs mesurées lors de la phase de post-traitement des données.

Cependant, comme il est impossible pour les participants de distinguer le bruit naturel provenant des appareils et le bruit artificiel provoqué par un attaquant, l'étude de la sécurité de ces protocoles consiste à la fois à évaluer au mieux le bruit minimum généré par les appareils et celui causé par l'attaque la plus efficace dont l'adversaire dispose.

Scarani *et al* décrivent en [22] un état de l'art de la sécurité des protocoles de Distribution Quantique de Clés en insistant sur l'aspect pratique des implémentations.

2.3.1 Les différentes stratégies d'un attaquant

La sécurité théorique d'un cryptosystème de Distribution Quantique de Clés repose sur l'assurance qu'un attaquant, en agissant sur les états quantiques pour en retirer de l'information, introduit des erreurs qui seront détectées par les participants. Mais en pratique, l'implémentation de ces cryptosystèmes n'est jamais parfaitement conforme au modèle de sécurité théorique et les imperfections des appareils utilisés laissent la possibilité à un attaquant de réaliser des attaques dites *zero-error attacks*, qui n'introduisent pas d'erreurs visibles.

Ces attaques sur l'implémentation, similaire aux attaques *par canaux auxiliaires* (ou *par canaux cachés*) déjà présentes dans la cryptographie classique, sont fréquemment regroupées dans la catégorie du *Quantum Hacking*.

Dans cette partie, nous décrirons les stratégies les plus fréquentes qu'un attaquant peut mettre en place en commençant par les stratégies d'attaque contre les cryptosystèmes théoriques dont on peut trouver un rappel détaillé dans la thèse d'Aurélien Bocquet en [23].

Nous donnerons ensuite quelques précisions sur l'implémentation de ces cryptosystèmes et sur les attaques de type *Quantum Hacking* qui peuvent permettre à un adversaire d'interagir avec les appareils sans être repéré, voire de récupérer totalement la clé secrète dans certains cas. Nous terminerons en exposant plusieurs stratégies de défense radicalement différentes contre le *Quantum Hacking* : la mise en place de contre-mesures adaptées au cas par cas et la certification des appareils utilisés par des méthodes de type *Device-Independence*.

2.3.1.1 Quelques définitions de sécurité

Définition 37 Sécurité calculatoire (*computational security*) :

Ce modèle de sécurité théorique assure la protection de l'algorithme de chiffrement contre un adversaire disposant de moyens de calculs limités. Cette puissance de calcul permise à l'adversaire permet alors de quantifier le niveau de sécurité que l'on souhaite obtenir. Cette sécurité est relative dans le sens où un progrès technologique futur peut permettre à un adversaire d'attaquer un système ancien dont la sécurité repose sur une puissance de calculs obsolète.

Définition 38 Sécurité inconditionnelle (*I-T security*) :

C'est le modèle de sécurité théorique le plus solide, qui suppose qu'un attaquant avec des moyens de calculs illimités ne peut récupérer aucune information sur le texte clair même s'il en connaît le chiffré. On l'appelle souvent *Information-Theoretic security* ou encore *perfect secrecy*.

A ce jour, le seul cryptosystème permettant ce niveau de sécurité théorique est le cryptosystème One-Time Pad (OTP).

Définition 39 Confidentialité persistante (*forward secrecy*) :

Cette propriété de sécurité garantit que la découverte par un adversaire de la clé secrète d'un participant ne compromet pas la sécurité des anciennes communications.

Remarque :

Il faut faire la distinction entre la confidentialité persistante qui concerne la compromission d'une clé et la compromission du cryptosystème sous-jacent. Dans le cas d'un cryptosystème dont la sécurité est calculatoire, même s'il assure la confidentialité persistante, un adversaire peut toujours stocker les échanges chiffrés et attendre une future cryptanalyse de l'algorithme de chiffrement qui lui permettrait de déchiffrer ces anciennes communications.

Définition 40 Quantum Bit Error Rate (QBER) :

Le QBER est le ratio du taux d'erreurs (bits non reçus ou erronés) sur le taux de bits reçus. En le calculant, on obtient des informations sur l'existence d'un attaquant et sur la quantité d'information potentiellement récupérée.

Le QBER dépend fortement des caractéristiques des appareils de mesure utilisés et du protocole considéré. Dans le cas du protocole BB84, l'équation du QBER décrite par Bacsardi *et al* dans [24] est la suivante :

$$\text{QBER} := P_{pol} + \frac{P_{dark} \times n}{\tau_{link} \times \eta \times 2 \times \mu}.$$

— P_{pol} : probabilité d'un photon arrivant sur le mauvais détecteur (1-2%),

— P_{dark} : probabilité d'un faux signal de photon (Si : 10-7% ; GaAs 10-5%),

— n : nombre de détecteurs,

— τ_{link} : taux de transmission,

— η : nombre de photons moyen par impulsion du signal,

— μ : sensibilité du détecteur.

2.3.1.2 Les modèles d'attaques théoriques

Définition 41 Attaques interception-réémission :
L'attaquant Eve ne dispose pas de mémoire quantique pour stocker les qudits. Elle déroute chaque qudit destiné à Bob et le mesure dans des bases, pas obligatoirement les mêmes que celles de Bob, avant de le transmettre à son destinataire.

Si les bases choisies sont les mêmes que celles d'Alice, Eve obtient toute l'information sur le bit secret sans perturber l'état qu'elle renvoie ensuite à Bob. Sinon, Eve n'obtient pas le bit secret et perturbe l'état renvoyé à Bob.

Définition 42 Attaques individuelles :
L'attaquant Eve peut stocker les qudits envoyés pas Alice dans une mémoire quantique mais ne peut attaquer chaque qudit qu'individuellement et avec la même stratégie pour tous. De plus, Eve doit mesurer ses états quantiques séparément avant le début des phases de correction d'erreur et d'amplification de confidentialité.

En revanche, elle peut attendre la phase de révélation des bases et choisir ses mesures en conséquence.

Définition 43 Attaques collectives :
Dans ces attaques qui généralisent les attaques individuelles, Eve doit employer la même stratégie d'attaque pour chaque qudit mais peut effectuer une mesure collective simultanée sur tous les états stockés en attendant après la phase de réconciliation, voire après la fin du protocole.

Définition 44 Attaques cohérentes :
L'attaquant Eve n'est soumis à aucune contrainte autre que le respect des lois de la physique quantique.

2.3.1.3 Les attaques de type *Quantum Hacking* et leurs contre-mesures

Bien que les familles générales d'attaques et leurs preuves de sécurités correspondantes soient souvent caractérisées en théorie, le passage à des implémentations pratiques ouvre la voie à une toute autre catégorie d'attaques qui tirent profit des failles des composants du système de QKD : le *Quantum Hacking*. Dans ce qui suit, on va donner une liste non exhaustive de quelques attaques connues et leurs contre-mesures associées.

Définition 45 L'attaque Cheval de Troie (*Trojan Horse attack*) :

Lors de cette attaque, l'adversaire Eve sonde les appareils d'Alice et Bob en envoyant puis collectant des signaux lumineux. Dans le cas des implémentations où le trajet de la lumière se fait en sens unique d'Alice vers Bob, une contre-mesure consiste à utiliser un isolateur optique. En cas de trajet dans les deux sens, on peut ajouter un détecteur additionnel pour surveiller le signal lumineux.

Définition 46 L'attaque *Fake State* :

Eve utilise diverses imperfections optiques dans les appareils de Bob et construit des impulsions lumineuses (les *faux états* contenant des valeurs de bits choisis par Eve) de telle sorte que Bob ne puisse plus distinguer les détections normales des fausses détections.

Exemple :

Lors d'une *detector blinding attack*, Eve émet une lumière vive dans les détecteurs de manière à les faire entrer dans le mode dit *linear mode operation*. Dans ce mode, ils ne sont plus sensibles aux impulsions de photons uniques mais uniquement aux impulsions de lumière forte. Eve contrôle alors totalement les détecteurs et peut produire des *clicks* à son gré en envoyant ces impulsions de lumière forte.

Une contre-mesure possible consiste à faire varier aléatoirement l'efficacité des détecteurs, comme proposé par Lim *et al* dans [25].

Définition 47 L'attaque *Photon Number Splitting* **:**

En théorie, les protocoles de QKD de la famille Prépare-et-Mesure utilisent des états transmis par des photons uniques mais, en pratique, les sources de photons uniques parfaites n'existent pas, du moins pas encore. Par exemple, la majorité des implémentations de BB84 utilisent à la place des sources produisant des états de type *phase-randomized weak coherent state pulses (WCPs)* préparés avec des lasers semi-conducteurs et des des atténuateurs calibrées.

Ces signaux ont typiquement un nombre de photon moyen de 0.1 ou plus, mais il arrive parfois qu'un signal contienne plusieurs photons préparés dans le même état quantique. Si un adversaire Eve effectue une attaque dite *Photon Number Splitting attack* sur ce signal multi-photon, il peut récupérer toute l'information sur cette partie de la clé sans générer une perturbation notable.

La production d'états à plusieurs photons résulte également en des protocoles de QKD plus lents, avec des taux de génération de clé de l'ordre de η^2, avec η la capacité du canal quantique.

Définition 48 La contre-mesure Decoy-State :

La technique du *decoy-state* décrite par Lo *et al* dans [26] permet à la fois de contrer l'attaque PNS et d'améliorer grandement le taux de génération de clé avec un taux linéaire en η.

Dans cette technique, au lieu d'envoyer des signaux de même intensité, la source (Alice) envoie des impulsions dont chaque intensité est aléatoirement choisie parmi un ensemble de valeurs de départ. L'une de ces intensités est choisie pour définir les états du signal tandis que les états d'intensités différentes correspondent à des leurres dits *decoy states*.

Après la phase de transmission, Alice dévoile à Bob les intensités de chaque impulsion. Eve ne pouvant distinguer entre les impulsions leurre et les impulsions du signal, elle devra attaquer toutes les impulsions de la même façon. Ainsi, les QBERs associés aux différents leurres permettent à Alice et Bob d'estimer la présence d'Eve.

Avec cette technique, les sources utilisées en pratique donnent des résultats presque aussi bons que les sources de photons uniques.

Autres exemples d'attaques selon les appareils visés :

De nombreuses autres attaques exploitant différents appareils sont possibles :

Attaque	Composant ciblé	Type de système attaqué
Time-shift	détecteur	commercial
Time information	détecteur	recherche
Detector-control	détecteur	recherche et commercial
Detector dead-time	détecteur	recherche
Channel calibration	détecteur	commercial
Phase-remapping	modulateur de phase	commercial
Faraday-mirror	miroir Faraday	théorique
Wavelength	beamsplitter	théorique
Phase information	source	recherche
Device calibration	oscillateur local	recherche

Remarque : Les attaques portant sur la source de photons sont moins critiques que celles portant sur les détecteurs car elles peuvent être prises en compte dans les modèles de sécurité, ce qui n'est pas le cas pour les autres attaques.

Stratégies de contre-mesures :

Pour remédier à ces attaques, on peut adopter trois stratégies différentes :

1. *Patchs de sécurité :* mise en place de contre-mesures adaptées au cas par cas selon les attaques découvertes.

2. *Certification des composants par Device-Independence (DI) :* les appareils utilisés par Alice et Bob sont traités comme des boites noires dont le fonctionnement interne est totalement inconnu. Le calcul de la violation d 'une inégalité de Bell leur permet de vérifier la présence des corrélations quantique et donc de certifier le comportement des appareils comme étant conforme au modèle attendu. Cette technique est actuellement difficilement réalisable car elle requiert d'utiliser des détecteurs ayant une efficacité de 80% minimum pour assurer un test de Bell conforme. De plus, les taux de génération de clé sont actuellement très faibles (de l'ordre de 10^{-10} bits par impulsion).

3. *Measurement Device-Independence (MDI) :* cette alternative à la Device-Independence, plus viable actuellement, permet à Alice et Bob d'effectuer de la QKD avec des appareils de mesure non sûrs, ce qui déplace les attaques sur la source au lieu des détecteurs. Elle permettrait d'atteindre des taux de clé presque

équivalents au *decoy-state* BB84 grâce à l'utilisation de détecteurs SNSPD atteignant 93% d'efficacité.

Quelques remarques sur la faisabilité des attaques en cas de liaison Bord/Sol :

Dans le cas de nos liaisons Bord/Sol, on considèrera que la source est placée au sol chez Alice et que le satellite joue le rôle de Bob.

Pour intercepter un photon lors d'une attaque de type interception-réémission, Eve doit être angulairement proche de Bob car l'intensité du faisceau décroit vite quand l'angle augmente, ce qui rend l'interception difficile dans le contexte d'une mission spatiale. Lors d'une attaque visant à aveugler les détecteurs du satellite, il faudrait qu'Eve dispose d'une source très puissante bien focalisée et placée à une distance proche d'Alice pour être dans le champ de vue de Bob.

De plus, l'accès aux appareils paraît difficile dans le cas d'un équipement embarqué, ce qui restreint également les possibilités sur le satellite lui-même.

2.4 Les inégalités de Bell et la sécurité des protocoles à intrication

Dans les protocoles de cryptographie quantique utilisant l'intrication, des inégalités mathématiques appelées *inégalités de Bell* peuvent permettre aux participants de vérifier si le protocole a été perturbé par une intervention externe (une attaque ou du bruit naturel) en calculant une valeur attendue dite *facteur de violation*.

En effet, certains états intriqués permettent d'obtenir des violations des inégalités de Bell, alors qu'obtenir une violation avec un état classique est impossible. La valeur de violation de l'inégalité sert donc à quantifier la distance entre le caractère quantique de l'état intriqué utilisé et le monde classique. Une intervention externe ajoute du bruit au système quantique et le rapproche d'un système classique, réduisant ainsi la possibilité d'obtenir une violation. Lorsqu'une trop grande quantité de bruit est ajoutée, aucune violation de l'inégalité n'est observée.

En particulier, certaines attaques ajoutent du bruit au système quantique. On peut donc définir un critère de sécurité contre ces attaques en choisissant une inégalité qui tolère un bruit inférieur au bruit minimum qu'elles provoquent. Ainsi, une absence de violation signifie que le protocole a subit un bruit suffisamment élevé pour avoir permis une attaque.

Comme chaque inégalité peut atteindre une valeur de violation maximale spécifique et que celle-ci est liée au bruit maximal toléré, le choix de l'inégalité joue un rôle important dans la sécurité du protocole.

Dans cette section, nous listons diverses inégalités de Bell utilisées dans des protocoles de cryptographie quantique. Nous décrivons d'abord l'inégalité CHSH en dimension 2 pour deux parties, puis l'inégalité CGLMP-d en dimension d pour deux parties. Lorsque $d = 3$, François Arnault a montré en [1] que l'inégalité CGLMP-3 est équivalente à l'inégalité CHSH-3 décrite par Chen *et al* en [27]. Nous introduisons ensuite les inégalités de Bell homogènes en dimension d pour n parties et nous explicitons le lien entre la violation de ces inégalités, la résistance au bruit des protocoles et leur sécurité contre une famille d'attaques appelées *attaques individuelles par clonage*.

2.4.1 Choix de bases pour les inégalités CGLMP-d

Dans cette thèse, on considère des observables à d issues notées $1, \omega, ..., \omega^{d-1}$, associées respectivement aux dits $0, ..., d-1$, avec ω la racine $d^{\text{ième}}$ de l'unité $\omega = e^{\frac{2i\pi}{d}}$.

Définition 49 Facteur de violation :
Le *facteur de violation* (ou *valeur de violation*) d'une inégalité de Bell se définit comme le quotient de sa valeur quantique sur sa borne classique :

$$v = \frac{\text{valeur quantique}}{\text{borne classique}}.$$

Nous allons maintenant rappeler la famille de bases utilisée dans le protocole NDEB décrit par Durt *et al* dans [28] pour obtenir une violation de l'inégalité CGLMP-d.

Définition 50 Choix de bases pour CGLMP-d :
Dans [28], Durt *et al* obtiennent des valeurs de violation pour l'inégalité CGLMP-d en choisissant une famille de bases qui correspond à des mesures de ditters paramétrés par les d-uplets de déphasages suivants :

$$(\theta_0, \theta_1, ..., \theta_{d-1}) \quad \text{où } \theta_k = \zeta^{ak} \text{ avec } \zeta = \mathrm{e}^{\frac{2i\pi}{4d}} \text{ pour } k = 0, ..., d-1 \text{ et pour un } a \text{ donné.} \quad (2.1)$$

Exemple 4 En particulier, dans le cas $d = 3$, ces quatre bases sont optimales dans le sens où elles maximisent la violation de l'inégalité CGLMP-3 [29, 30, 31].

Elles correspondent à des mesures de tritters [2, 32, 8] paramétrés par les d-uplets de déphasages $(1, \theta, \theta^2)$ où θ est une puissance de $\zeta = \mathrm{e}^{\frac{2i\pi}{12}}$.

On peut les schématiser comme suit :

$A_1 : (1, 1, 1)$
$A_2 : (1, \zeta^2, \zeta^4)$
$B_1 : (1, \zeta, \zeta^2)$
$B_2 : (1, \zeta^{-1}, \zeta^{-2})$

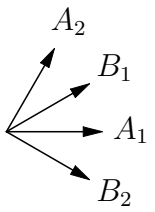


Figure 2.1 – Représentation des quatre bases optimales pour CHSH-3

Nous allons maintenant présenter diverses inégalités de Bell présentes dans la littérature.

2.4.2 Inégalités de Bell pour deux parties

Considérons le cas $n = 2$. Les observables utilisées par les deux parties Alice et Bob sont notées respectivement A_i et B_j pour des indices i and j donnés. Nous utilisons les fonctions de corrélations introduites par Mattle *et al.* dans [8] :

$$E(A_i B_j) = \sum_{a,b=1,\omega,\ldots,\omega^{d-1}} P(A_i = a, B_j = b)\, ab.$$

2.4.2.1 Inégalité CHSH en dimension 2

Nous considérons deux parties Alice et Bob utilisant des systèmes quantiques en dimension $d = 2$, appelés *qubits*. Alice choisit entre les mesures correspondant aux observables A_0, A_2 et Bob entre celles correspondant aux observables B_1, B_3. Ces observables ont comme issues les valeurs $1, -1$ associées respectivement aux bits $0, 1$.

On pose le polynôme T défini par :

$$T := A_0B_1 + A_0B_3 + A_2B_1 - A_2B_3.$$

Supposons qu'on se trouve dans un contexte de physique classique pour lequel chaque mesure des A_i et B_j donne comme issue 1 ou -1. Il y a seize 2-uplets possibles d'issues et, en remplaçant ces 2-uplets dans l'inégalité CHSH, on obtient obligatoirement $T \in \{-2, 2\}$. En considérant l'espérance mathématique $E(T)$, on trouve des bornes classiques -2 et 2.

L'inégalité CHSH exprimée en terme de fonctions de corrélations s'écrit donc :

$$-2 \leqslant E(T) \leqslant 2 \tag{2.2}$$

avec $E(T) = E(A_0B_1) + E(A_0B_3) + E(A_2B_1) - E(A_2B_3)$.

Pour deux qubits intriqués, les mesures devraient donc vérifier $|E(T)| \leqslant 2$. Or la quantité T expérimentale vérifie :

$$|E(T)| \leqslant 2\sqrt{2}$$

Ainsi, certains états intriqués dépassent les bornes classiques et provoquent une violation de l'inégalité CHSH. Cette borne $2\sqrt{2}$ est en particulier atteinte par les états maximalement intriqués pour lesquels on obtient $v_{\text{CHSH}} = \frac{2\sqrt{2}}{2} = \sqrt{2}$.

2.4.2.2 Inégalité CGLMP-d en dimension d

Dans [33], Collins *et al* utilisent les fonctions de probabilités conjointes suivantes :

$$P(A_a = B_b + k) := \sum_{j=0}^{d-1} P(A_a = j, B_b = j + k \pmod d). \tag{2.3}$$

Ils généralisent ensuite l'inégalité CHSH pour qubits à une famille d'inégalités de Bell en dimension d, souvent appelée CGLMP-d dans la littérature. En terme de fonctions de probabilités, l'inégalité CGLMP-d en dimension d s'écrit :

$$I_d \leqslant 2$$

$$\text{où} \quad I_d := \sum_{k=0}^{[d/2]-1} (1 - \frac{2k}{d-1})\{[P(A_0 = B_1 + k) + P(B_1 = A_2 + k + 1) + P(A_2 = B_3 + k) + P(B_3 = A_0 + k)] - [P(A_0 = B_1 - k - 1) + P(B_1 = A_2 - k) + P(A_2 = B_3 - k - 1) + P(B_3 = A_0 - k - 1)]\}. \tag{2.4}$$

Dans [33], Collins *et al* calculent également la valeur quantique maximale atteinte par cette famille d'inégalités :

$$I_d(QM) := 4d \sum_{k=0}^{[d/2]-1} (1 - \frac{2k}{d-1})(q_k - q_{-(k+1)}) \qquad \text{avec} \quad q_k = 1/(2d^2 \sin^2[\frac{\pi(k + \frac{1}{4})}{d}]).$$

Ainsi, ils calculent explicitement ces valeurs pour $d = 3, 4$ et estiment la valeur asymptotique pour $d \to \infty$:

d	3	4	∞
$I_d(QM)$	2.873	2.896	2.698

Exemple 5 : Inégalité CHSH-3 en dimension 3

Nous considérons deux parties Alice et Bob utilisant des systèmes quantiques en dimension 3, appelés *qutrits*. Les observables utilisées par les deux parties Alice et Bob sont notées respectivement par A_i et B_j pour des indices i and j donnés.

On utilisera également les fonctions de corrélation introduites par dans Mattle *et al* dans [8], pour le cas $d = 3$:

$$E(A_i B_j) = \sum_{a,b=1,\omega,\omega^2} P(A_i = a, B_j = b)\, ab.$$

Dans [33], Collins *et al* donnent la description de l'inégalité I_3 suivante pour le cas $d = 3$:

$$\begin{aligned} & I_3 \leqslant 2 \\ \text{où } I_3 :=& [P(A_0 = B_1) + P(B_1 = A_2 + 1) + P(A_2 = B_3) + P(B_3 = A_0)] \\ & - [P(A_0 = B_1 - 1) + P(B_1 = A_2) + P(A_2 = B_3 - 1) + P(B_3 = A_0 - 1)]\}. \end{aligned} \tag{2.5}$$

Dans [1], François Arnault montre que cette inégalité est équivalente à l'inégalité CHSH-3 décrite par Chen *et al* dans [27] en terme de fonctions de corrélations :

$$I_3 \leqslant 2$$

$$\begin{aligned} \text{où } I_3 = & \operatorname{Re}\big(E(A_0B_1) + E(A_0B_3) - E(A_2B_1) + E(A_2B_3)\big) \\ & + \tfrac{1}{\sqrt{3}}\operatorname{Im}\big(E(A_0B_1) - E(A_0B_3) - E(A_2B_1) + E(A_2B_3)\big). \end{aligned}$$

L'état maximalement intriqué pour $d = 3$ décrit en (1.10) et les bases optimales pour CHSH-3 décrites dans la Figure 2.1 permettent d'obtenir un facteur de violation de CHSH-3 égal à $v_{\text{CHSH}-3} = (6 + 4\sqrt{3})/9 \simeq 1.436$.

2.4.3 Inégalités de Bell homogènes en dimension d pour n parties

Dans le Chapitre 4, nous proposons d'exploiter les hautes valeurs de violations atteintes par les inégalités de Bell homogènes en dimension d pour n parties, avec $d \geqslant 3$ et $n \geqslant 2$, introduites par François Arnault en [1], pour obtenir des protocoles plus résistants au bruit que les protocoles actuels.

Ces inégalités font intervenir des polynômes dits *homogènes*, c'est-à-dire des polynôme en plusieurs indéterminées et dont tous les monômes non nuls sont de même degré.

Soient n parties, chacune disposant de deux observables notées A_i et B_i dont les issues a_i et b_i sont des éléments de $\mathfrak{U} = \{1, \omega, ..., \omega^{d-1}\}$. Les observables A_i commutent entre

elles, de même que les B_i. En revanche, les observables A_i ne commutent pas avec les B_i. D'après [1], on décrit un polynôme de Bell homogène en dimension d pour n parties par :

$$P_f = \sum_{r \in \mathbb{Z}_d^n} \widehat{f}(r) \prod_{i=1}^{n} A_i^{d-1-r_i} B_i^{r_i}. \tag{2.6}$$

Une inégalité de Bell homogène en dimension d pour n parties s'écrit :

$$\mathrm{Re}\left(\frac{\tau}{d^n \cos(\frac{\pi}{d})} \sum_{r \in \mathbb{Z}_d^n} \widehat{f}(r) E(a^r)\right) \leqslant 1 \tag{2.7}$$

où $\quad \tau = \mathrm{e}^{\frac{i\pi}{d}}, \quad a^r = \prod_{i=1}^{n} a_i^{d-1-r_i} b_i^{r_i} \quad$ et $\quad f : \mathbb{Z}_d^n \to \mathfrak{U}.$

En remplaçant les valeurs classiques A_i et B_i par les opérateurs quantiques X et Z décrits en 1.4, les opérateurs de Bell associés aux inégalités de Bell homogènes décrites précédemment s'écrivent :

$$Q_f = \sum_{r \in \mathbb{Z}_d^n} \widehat{f}(r) \bigotimes_{i=1}^{n} X^{d-1-r_i} Z^{r_i}. \tag{2.8}$$

Une caractéristique des inégalités de Bell homogènes est que P_f fait intervenir des produits de valeurs classiques (par exemple $A_1^3 A_2$, $A_1^2 A_2^2$ et $A_1 A_2^3$ pour les mesures d'une partie dans le cas $d = 5$) qui deviennent incompatibles quand considérées en tant qu'observables quantiques, c'est-à-dire qu'on ne peut mesurer les valeurs de ces deux observables simultanément. Les issues de ces produits d'observables ne peuvent donc pas résulter du produit des issues des observables.

Dans la Proposition 7, nous avons montré que si nous utilisons les observables unitaires Z_Θ définies en (1.5) en tant que A_i, le produit est également une observable unitaire dont les issues s'obtiennent avec une unique mesure. Nous en avons conclu qu'il est possible d'effectuer cette "mesure produit" grâce à un ditter spécifique et une détection dans la base canonique suivant $Z^\dagger$.

Soient deux parties nommées Alice et Bob et disposant respectivement des valeurs classiques A_i et B_i pour $i = 1, .., d-1$. Les produits de valeurs classiques $A_1^u A_2^v$ pour $u = 0, ..., d-1$ et $v = d-u-1$ pour Alice doivent être remplacées par les produits d'observables quantiques $Z^\dagger_{\Gamma_{uv_A}}$ comme décrit dans la Proposition 7. De la même manière, Bob doit utiliser les observables $Z^\dagger_{\Gamma_{uv_B}}$.

Exemple 6 Soit $d = 3$, on a alors $(u, v) \in \{(2, 0), (1, 1), (0, 2)\}$.

Les valeurs classiques A_1^2, A_2^2 et leur produit A_1A_2 pour Alice doivent être remplacés par les observables quantiques :

$$Z_{\Theta_A}^\dagger, \quad Z_{\Gamma_{11_A}}^\dagger, \quad Z_{\Lambda_A}^\dagger.$$

Les paramètres de l'observable $Z_{\Gamma_{11_A}}^\dagger$ dépendent ces paramètres des observables Z_{Θ_A} et Z_{Λ_A} d'après la Proposition 7. De la même manière, Bob doit remplacer ses valeurs classiques B_1^2, B_2^2 et leur produit B_1B_2 par les observables quantiques :

$$Z_{\Theta_B}^\dagger, \quad Z_{\Gamma_{11_B}}^\dagger, \quad Z_{\Lambda_B}^\dagger.$$

Un état quantique normalisé $|\psi\rangle$ permet d'obtenir une violation d'une inégalité de Bell homogène s'il *ne satisfait pas* la condition :

$$\mathrm{Re}\big(\frac{\tau}{d^n\cos(\frac{\pi}{d})}\langle\psi|\,Q_f\,|\psi\rangle\big) \leqslant 1 \qquad \text{pour } \tau = \mathrm{e}^{\frac{i\pi}{d}}. \tag{2.9}$$

Ainsi, après avoir substitué les observables quantiques des n participants aux valeurs classiques dans un polynôme de Bell P_f, l'état $|\psi\rangle$ permet donc d'obtenir une violation de l'inégalité de Bell homogène associée à l'opérateur de Bell Q_f avec une valeur de violation $v \geqslant 1$ si il vérifie :

$$\frac{1}{d^n\cos(\frac{\pi}{d})}\mathrm{Re}(\langle\psi|\,\tau Q_f\,|\psi\rangle) = v \qquad \text{pour } \tau = \mathrm{e}^{\frac{i\pi}{d}}. \tag{2.10}$$

2.4.4 Rôle des inégalités de Bell dans la sécurité théorique des protocoles basés sur l'intrication

La violation d'une inégalité de Bell peut être liée à la fois à la sécurité d'un protocole de Distribution Quantique de Clés basé sur l'intrication et à sa résistance au bruit. Dans cette section, on considère un protocole quelconque effectuant des tests de violation d'une inégalité de Bell.

En calculant la valeur de violation v associée à cette inégalité, nous décrivons un critère pour assurer la sécurité du protocole contre la famille d'attaques individuelles appelée *attaques par clonage*. Nous expliquons également comment optimiser la sécurité et la résistance au bruit grâce au choix judicieux d'une inégalité de Bell.

Supposons que deux participants, Alice et Bob, tentent d'établir une clé secrète à l'aide d'un protocole de Distribution Quantique de Clés, et qu'un adversaire Eve tente de récupérer cette clé sans être détecté en effectuant une attaque individuelle par clonage optimal, dont on va maintenant donner une description.

2.4.4.1 Attaques individuelles par clonage :

Une attaque par clonage utilise un cloneur pour copier un état d'entrée. Or, en physique quantique, il existe un théorème appelé *théorème d'impossibilité du clonage quantique* démontré par Wooters *et al* [34] en 1982 et stipulant qu'il est impossible de copier parfaitement un état quantique inconnu.

D'après ce théorème, l'état obtenu en sortie d'un cloneur est imparfait et le but d'Eve est de fabriquer un cloneur optimal dans le sens où ce cloneur copie un ensemble spécifique d'états le plus fidèlement possible, c'est-à-dire avec la plus faible quantité d'erreurs possible. Eve fabrique donc un cloneur optimal pour les états des bases utilisées dans le protocole à attaquer.

Selon les propriétés de l'état d'entrée ou la famille dont fait partie le cloneur, l'état peut être reproduit avec une certaine fidélité F_A définie par Durt *et al.* dans [28] par

$$F_A = \langle\psi|\,\rho\,|\psi\rangle \tag{2.11}$$

où $|\psi\rangle$ est l'état initial et ρ la matrice densité du clone obtenu.

Dans leur article [28], Durt *et al* introduisent et décrivent une attaque par clonage optimal qui utilise un cloneur pour qudit dit "phase-covariant". Ce cloneur agit identiquement sur chaque état des bases décrites en (2.1). Ces états sont tous copiés avec la même fidélité F_A selon la valeur de d :

d	3	4	5	6	7	8	9	∞
F_A	0.7753	0.7342	0.7080	0.6898	0.6762	0.6657	0.6573	0.5

Le facteur de violation comme critère de sécurité

Nous allons maintenant expliquer la relation directe entre la violation d'une inégalité de Bell judicieusement choisie et la sécurité du protocole contre la famille d'attaques par clonage optimal décrites précédemment.

Dans ce contexte, le facteur de violation est considéré comme très important pour la sécurité d'un protocole de Distribution Quantique de Clés.

Canal quantique dépolarisant :

Le bruit présent sur un canal quantique dit *à dépolarisation* ou *dépolarisant*, qu'il soit naturel ou provoqué par un attaquant, est modélisée par le remplacement de l'état intriqué initial par le mélange suivant :

$$N\frac{I}{d} + (1-N)\left|\psi\right\rangle\left\langle\psi\right| \tag{2.12}$$

où N est la proportion de bruit. Ce canal transforme l'état d'entrée $|\psi\rangle$ en un état complètement mixte, avec une probabilité N et ne fait rien avec une probabilité $1-N$.

La présence de bruit fait décroître le facteur de violation jusqu'à $(1-N)v$ et la violation de l'inégalité ne peut plus servir de critère de sécurité lorsque l'intrication de l'état initial ne peut plus être détectée.

Suivant ce critère, Durt *et al* précisent dans [28] qu'un protocole est résistant au bruit jusqu'à un seuil :

$$N = 1 - 1/v. \tag{2.13}$$

Fidélité dans un canal dépolarisant :

Lorsqu'on utilise un canal dépolarisant décrit par (2.12), la fidélité (comme définie dans (2.11)) entre l'état d'entrée $|\psi\rangle$ et l'état de sortie est donnée par :

$$F_N = \left\langle\psi\right|\rho'\left|\psi\right\rangle = -\frac{d-1}{d}N + 1$$

où $\rho' = N\frac{I}{d} + (1-N)\left|\psi\right\rangle\left\langle\psi\right|$.

La présence de bruit N ne supprime pas le caractère non classique des corrélations tant que la quantité de bruit reste sous le seuil donné par (2.13). Ainsi, il est possible d'utiliser un canal bruité pour faire de la Distribution Quantique de Clés si la fidélité de ce canal satisfait :

$$F_N > \frac{d-1}{dv} + \frac{1}{d}. \tag{2.14}$$

Critère de sécurité :

Supposons que l'adversaire Eve utilise un cloneur optimal qui copie un état d'entrée avec une fidélité F_A et dont l'action sur le canal est indistinguable de celle provoquée par un bruit naturel.

Les attaques de Eve ne brisent pas l'intrication tant que $F_A \geqslant F_N$. Ainsi, la sécurité du protocole contre les attaques individuelles par clonage est garantie si on a $\frac{d-1}{dv} + \frac{1}{d} > F_A$, ce qui est équivalent à $v < v_{\text{borne}}$ avec $v_{\text{borne}} = \frac{d-1}{dF_A - 1}$.

En remplaçant F_A pour chaque $d = 3, 4, 5$, on obtient les conditions suivantes :

d	3	4	5	6	7	8	9	∞
v_{borne}	1.508	1.549	1.575	1.593	1.607	1.618	1.627	2

Tableau 2.2 – Critère de sécurité contre les attaques individuelles par clonage

2.5 Etat-de-l'art de la sécurité des protocoles les plus courants

Dans cette section, nous donnons un résumé rapide de la sécurité des protocoles décrits précédemment : les protocoles BB84, E91 et BBM92. Nous mentionnons également les nombreux facteurs influenant les preuves de sécurité, qui sont notamment dûs à la distance entre les modèles de sécurité théoriques supposés parfaits et les situations pratiques en cas d'implémentation avec des appareils imparfaits. Ces divers facteurs, ainsi que l'absence de standardisation qui est en cours au moment de cette thèse, rendent difficile une évaluation exhaustive de la sécurité des protocoles.

2.5.1 Résumé sur la sécurité des protocoles BB84 et BBM92

Sécurité du protocole BB84

Dans l'article originel de Bennett et Brassard, pour vérifier la sécurité sur un canal quantique non bruité, Alice et Bob révèlent une partie des issues retenues pour estimer le taux d'erreurs entre leurs deux chaînes de bits. Si les issues sacrifiées sont identiques, Alice et Bob peuvent ensuite appliquer des techniques de correction d'erreurs et d'amplification de confidentialité sur le reste de leurs bits pour dériver la clé secrète commune.

La sécurité inconditionnelle du protocole BB84 a été prouvée dans le cas idéal d'un environnement non bruité par Shor *et al* en 2000 dans [35].

Sécurité du protocole BBM92

L'intérêt porté au protocole BBM92, équivalent de BB84 avec intrication, s'explique en partie par le fait qu'il est généralement plus facile d'étudier la sécurité des protocoles basés sur l'intrication plutôt que celle des protocoles de type Prépare-et-Mesure. Sous certaines conditions, on peut donc tirer parti d'une preuve de sécurité concernant un protocole à intrication pour en conclure sur la sécurité de son équivalent de type Prépare-et-Mesure.

A titre d'exemple, une preuve de sécurité en environnement bruité basée sur les codes correcteurs d'erreur s'appliquant à la fois au protocole BB84 et au protocole BBM92 a été présentée par P.W. Shor et J. Preskill en 2000 dans [35].

Toutefois, si cette équivalence est valide dans le cas d'un environnement idéal non bruité, elle ne l'est pas toujours pour un environnement bruité comme expliqué par Sharma *et al* dans [36]. En particulier, Sharma *et al* décrivent dans [36] l'action d'un canal quantique bruité sur les qubits intriqués selon le type de bruit présent dans le canal quantique.

La sécurité inconditionnelle du protocole BBM92 a été prouvée dans le cas idéal d'un environnement non bruité par H. Inamori *et al* dans [37]. Dans le cadre d'un environnement bruité, les participants ne peuvent différencier le bruit provoqué par une attaque du bruit déjà présent dans le canal quantique et ils cherchent à évaluer et à réduire l'information que l'attaquant a de la clé en utilisant des techniques comme la correction d'erreur puis l'amplification de confidentialité.

La sécurité inconditionnelle du protocole BBM92 n'est pas prouvée en environnement bruité. Les preuves de sécurité dépendent alors de l'implémentation du protocole, du type de bruit présent et des familles d'attaques considérées.

De plus, il est rare que les appareils utilisés lors d'expériences correspondent exactement à leur modèle théorique et la sécurité du protocole BBM92 peut également varier selon la manière dont on l'implémente. Ainsi, Ma *et al*, Koashi *et al* et Cai *et al* évaluent dans [38], [39] et [40] les possibilités d'obtenir la sécurité inconditionnelle du protocole BBM92 pour trois situations d'implémentation avec des appareils imparfaits.

2.5.2 Résumé sur la sécurité du protocole E91

Violation de l'inégalité CHSH :

Dans le cas d'un protocole basé sur l'intrication, les participants peuvent réaliser des tests de sécurité faisant intervenir une inégalité de Bell pour déterminer si il y a potentiellement eu espionnage.

Dans le protocole E91, lorsque leurs choix de bases vérifient $a \neq b$, Alice et Bob peuvent en effet utiliser une partie de leurs résultats pour calculer une ou plusieurs violations de l'inégalité CHSH en dimension 2 décrite en (2.2).

Si les valeurs de violations calculées dépassent 1, ils peuvent dériver une clé secrète avec les bits partagés lors du protocole. Dans le cas contraire, les bits partagés sont potentiellement compromis et donc inutilisables. Le protocole doit alors être recommencé du début.

Exemple 7 Violation de l'inégalité CHSH dans le protocole E91
On peut prendre l'exemple de la violation de l'inégalité CHSH pour les choix de bases décrits précédemment dans le cadre du protocole E91.

Pour la configuration 1 (resp. 2), l'inégalité CHSH s'exprime avec le polynôme T_1 (resp. T_2) suivant :

$$T_1 = A_0B_1 + A_0B_3 + A_2B_1 - A_2B_3 \quad (\text{resp.} \quad T_2 = A_1B_0 + A_1B_2 + A_3B_0 - A_3B_2).$$

Les choix de bases précédents et l'état $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ permettent d'obtenir deux violations de l'inégalité CHSH avec T_1 et T_2, chacune atteignant une même valeur $v_{\text{CHSH}} \simeq 1,414 \geqslant 1$.

Les différentes situations du protocole E91 peuvent alors se résumer dans le tableau suivant :

	B_0	B_1	B_2	B_3
A_0	k	c_1		c_1
A_1	c_2	k	c_2	
A_2		c_1	k	c_1
A_3	c_2		c_2	k

k : Alice et Bob obtiennent des bits de clé.

c_1 et c_2 : Alice et Bob obtiennent des valeurs pour vérifier la violation de CHSH.

Tableau 2.3 – Résumé du protocole E91

Ainsi, sur les $4 \times 4 = 16$ choix de mesures possibles, on a :

- 4 choix résultant en un bit de clé (**25**%),
- 8 choix intervenant dans la vérification des inégalités CHSH (**50**%),
- 4 choix inutilisés (**25**%).

Conclusion :

Dans ce chapitre, nous avons explicité le fonctionnement des protocoles de Distribution Quantique de Clés en les séparant en deux familles : les protocoles Prépare-et-Mesure et les protocoles à intrication. Nous avons ensuite mentionné les différents outils d'implémentation de ces protocoles et leurs caractéristiques associées, puis nous avons longuement traité les modèles de sécurité théorique et les failles d'implémentation. Nous avons décrits en détail les protocoles les plus courants, en particulier les protocoles BB84, BBM92 et E91 et nous avons listé des éléments importants concernant leur sécurité.

Nous avons aussi souligné l'importance des inégalités de Bell dans la sécurité des protocoles à intrication et nous avons rappelé certaines de ces inégalités, dont l'inégalité CHSH en dimension 2 pour deux parties, l'inégalité CGLMP-d (ou CHSH-d) en dimension d pour deux parties et les inégalités de Bell homogènes en dimension d pour n parties. Finalement, nous avons présenté le lien entre la violation de ces inégalités, la résistance au bruit des protocoles et leur sécurité contre les attaques individuelles par clonage.

Chapitre 3 :

Etude théorique des inégalités de Bell homogènes en dimension d

Dans la première section de ce chapitre, nous étudierons une inégalité en dimension 3 à deux parties et à 3 mesures par partie décrites par Ji *et al.* dans [41], puis réexaminée par Liang *et al.* dans [42]. En reformulant ces inégalités, nous expliciterons leur lien avec les inégalités de Bell homogènes en dimension 3 pour deux parties et à deux mesures par partie et nous recalculerons leurs bornes classiques. La valeur de violation quantique étant inchangée, ces nouvelles bornes classiques nous permettrons d'obtenir de meilleures valeurs de violation pour les inégalités de Ji *et al.* et Liang *et al.*.

La seconde section sera consacrée à la dérivation d'une borne supérieure sur les valeurs de violation des inégalités de Bell homogènes en dimension d pour n parties.

3.1 Comparaison avec des inégalités préexistantes

On considère deux parties Alice et Bob utilisant des systèmes quantiques en dimension $d = 3$, et on pose $\omega = e^{\frac{2i\pi}{3}}$ et $\zeta = e^{\frac{2i\pi}{3}}$ les racines troisième et neuvième de l'unité respectivement. Soient les observables A_0, A_1, A_2 pour Alice et B_0, B_1, B_2 pour Bob dont on note les issues $1, \omega, \omega^2$.

Dans cette section, on utilisera les observables suivantes, dont la matrice identité $\mathbb{I}$ et les deux matrices de Pauli Z et X en dimension 3 décrites en (1.4) :

$$\mathbb{I} = \sum_{k=0}^{2} |k\rangle \langle k| \qquad Z = \sum_{k=0}^{2} \omega^k |k\rangle \langle k|$$
$$X = \sum_{k=0}^{2} |k+1\rangle \langle k| \qquad P = \sum_{k=0}^{2} \zeta^{-k} |k\rangle \langle k|$$

En physique quantique, lorsqu'on se place dans le cadre du réalisme local décrit par les définitions 25 et 26, la valeur obtenue en effectuant une mesure est pré-existante et peut dépendre d'une variable locale cachée. Dans la suite de ce chapitre, on suppose que le résultat d'une mesure A_i (resp. B_j) dans un contexte réaliste local avec une une variable locale cachée λ se note $\omega^{a_i(\lambda)}$ (resp. $\omega^{b_j(\lambda)}$).

3.1.1 Inégalité de Ji *et al.* à trois mesures par partie

Ji *et al.* introduisent dans [41] une inégalité de Bell pour qutrits à trois mesures par partie définie par les bornes non optimales

$$-\frac{9}{2} \leqslant \mathrm{B_{Ji}} \leqslant \frac{9}{2} \tag{3.1}$$

et par la fonction de corrélations

$$\mathrm{B_{Ji}} = \frac{1}{2}\sum_{n=1}^{2}\sum_{i,j=0}^{2}\omega^{nij}A_i^n B_j^n \tag{3.2}$$

Les auteurs déterminent des bornes supérieures et inférieures pour l'inégalité (3.1). Dans une description réaliste locale dépendant d'une variable locale cachée λ, ils réécrivent la fonction de Bell (3.2) comme suit :

$$\begin{aligned}\mathrm{B_{Ji}}(\lambda) &= \frac{1}{2}\sum_{n=1}^{2}\sum_{i,j=0}^{2}\omega^{nij}A_i^n(\lambda)B_j^n(\lambda)\\ &= \frac{1}{2}\sum_{n=1}^{2}\sum_{i,j=0}^{2}\omega^{nij}\omega^{na_i(\lambda)}\omega^{nb_j(\lambda)}\\ &= \frac{1}{2}\sum_{n=1}^{2}\sum_{i,j=0}^{2}\omega^{n(ij+a_i(\lambda)+b_j(\lambda))}\end{aligned}$$

En posant $3\delta_x = \sum_{n=0}^{2}\omega^{nx} = \sum_{n=1}^{2}\omega^{nx}+1$ où $\delta_x = 1$ si $x \equiv 0 \pmod 3$ et $\delta_x = 0$ sinon, les auteurs Ji *et al.* obtiennent :

$$\begin{aligned}\mathrm{B_{Ji}}(\lambda) &= \frac{1}{2}\sum_{i,j=0}^{2}(3\delta_{ij+a_i(\lambda)+b_j(\lambda)}-1)\\ &= \frac{1}{2}(3\sum_{i,j=0}^{2}\delta_{ij+a_i(\lambda)+b_j(\lambda)}-9)\\ &= \frac{3}{2}(\sum_{i,j=0}^{2}\delta_{ij+a_i(\lambda)+b_j(\lambda)}-3)\end{aligned}$$

Les valeurs extrémales de $\sum_{i,j=0}^{2}\delta_{ij+a_i(\lambda)+b_j(\lambda)}$ sur λ sont notées :

$$\Delta_{\min} = \mathrm{Min}_\lambda(\sum_{i,j=0}^{2}\delta_{ij+a_i(\lambda)+b_j(\lambda)})$$

$$\Delta_{\max} = \mathrm{Max}_\lambda(\sum_{i,j=0}^{2}\delta_{ij+a_i(\lambda)+b_j(\lambda)})$$

Ainsi, les bornes supérieures et inférieures sont données par :

$$\frac{3}{2}(\Delta_{\min}-3) \leqslant \mathrm{B_{Ji}}(\lambda) \leqslant \frac{3}{2}(\Delta_{\max}-3) \tag{3.3}$$

En effectuant une recherche exhaustive sur toutes les stratégies locales possibles, les auteurs Ji *et al.* obtiennent les valeurs extrémales :

$$\Delta_{\min} = 0 \quad \text{and} \quad \Delta_{\max} = 6$$

ce qui donne l'inégalité (3.1).

Ji *et al.* déterminent également des paramètres maximisant la violation de leur inégalité par la mécanique quantique. Ils utilisent les trois bases sans biais décrites par les observables suivantes, pour Alice mesurant les observables A_i et Bob mesurant les observables B_i avec $i = 0, .., 2$:

$$\begin{aligned} A_0 &= X & B_0 &= X \\ A_1 &= \omega^2 XZ & B_1 &= XZ^2 \\ A_2 &= XZ^2 & B_2 &= \omega^2 XZ \end{aligned}$$

et l'état optimal $|\psi\rangle = I \otimes P\,|\psi_{\mathrm{GHZ}_2}\rangle$, avec $|\psi_{\mathrm{GHZ}_2}\rangle$ un état maximalement intriqué pour qutrits décrit en (1.10).

Avec ces paramètres, les auteurs obtiennent une valeur quantique maximale $\langle\psi|\,\mathrm{B_{Ji}}\,|\psi\rangle \simeq 5.117$ qui donne une valeur de violation $v_{\mathrm{Ji}} \simeq 5.117 \times \frac{2}{9} \simeq 1.137$.

3.1.2 Réexamination de l'inégalité de Ji *et al.*

Liang *et al.* réexaminent dans [42] les inégalités de Bell de Ji *et al.* et recalculent certaines bornes incorrectes pour $d \geqslant 5$. Au lieu d'utiliser des corrélations, ils choisissent d'exprimer leurs fonctions de Bell en termes de probabilités conjointes considérant simultanément les deux variables A et B.

Considérons deux parties Alice et Bob utilisant des systèmes quantiques en dimension $d = 3$. On pose $\omega = e^{\frac{2i\pi}{3}}$ et $\zeta = e^{\frac{2i\pi}{9}}$ les racines troisième et neuvième de l'unité respectivement. Soient les observables A_0, A_1, A_2 pour Alice et B_0, B_1, B_2 pour Bob, dont on note les issues $1, \omega, \omega^2$.

Pour $i, j, k, l = 0, 1, 2$, on note $\mathrm{P}^{kl}_{AB}(i, j)$ la probabilité conjointe qu'Alice obtienne l'issue ω^i en effectuant la mesure A_k et que Bob obtienne l'issue ω^j en effectuant la mesure B_l.

Posons la fonction de Bell probabiliste :

$$\mathrm{B_{Liang}} = \frac{1}{9} \sum_{i,j,k,l=0}^{2} \delta_{ij+k+l} \mathrm{P}^{kl}_{AB}(i, j) = \frac{1}{27}(\mathrm{B_{Ji}} + 9) \tag{3.4}$$

L'inégalité de Liang *et al.* s'écrit alors :

$$0 \leqslant \mathrm{B}_{\mathrm{Liang}} \leqslant \frac{2}{3} \tag{3.5}$$

En effet, les auteurs trouvent les bornes :

$$\frac{1}{9}\Delta_{\min} \leqslant \mathrm{B}_{\mathrm{Liang}} \leqslant \frac{1}{9}\Delta_{\max} \tag{3.6}$$

Dans leur article, ils observent que leurs valeurs extrémales $\Delta_{\min}$ et $\Delta_{\max}$ sont les mêmes dans le cas des qutrits que dans (3.1). En conséquence, pour $\Delta_{\min} = 0$ et $\Delta_{\max} = 6$, ils obtiennent l'inégalité (3.5).

Comme attendu, leur inégalité est maximisée par les mêmes bases et le même état que (3.1), ce qui donne une valeur quantique maximale :

$$\langle\psi|\,\mathrm{B}_{\mathrm{Liang}}\,|\psi\rangle \simeq 0.7124 \simeq \frac{1}{27}(2 \times 5.117 + 9) \simeq \frac{1}{27}(\langle\psi|\,\mathrm{B}_{\mathrm{Ji}}\,|\psi\rangle + 9) \tag{3.7}$$

Toutefois, le rapport entre la valeur quantique et les bornes classiques étant différent, Liang *et al.* obtiennent une autre valeur de violation $v_{\mathrm{Liang}} \simeq 0.7124 \times \frac{3}{2} \simeq 1.069$.

3.1.3 Lien avec les inégalités de Bell homogènes

Pour faire le lien entre les inégalités de Bell homogènes décrites au Chapitre 2 et les deux inégalités décrites précédemment, il nous faut faire remarquer que le choix d'utiliser ces trois bases sans biais ajoute les contraintes de multiplicité suivantes sur les opérateurs d'Alice et Bob :

$$A_2^2 = A_0 A_1 \qquad B_1^2 = B_0 B_2 \tag{3.8}$$

Avec ces contraintes, nous considérons les inégalités de Bell homogènes :

$$-2 \leqslant -\frac{2}{9}\mathrm{Re}(\mathrm{T}_1) \leqslant 1 \tag{3.9}$$

$$-2 \leqslant -\frac{2}{9}\mathrm{Re}(\mathrm{T}_2) \leqslant 1 \tag{3.10}$$

$$-2 \leqslant -\frac{2}{9}\mathrm{Re}(\mathrm{T}_3) \leqslant 1 \tag{3.11}$$

avec les polynômes homogènes suivants :

$$\begin{aligned}\mathrm{T}_1 = 3\ [\ & E(A_0^2B_0^2) + E(A_0^2B_1^2) + E(A_0^2B_2^2) + E(A_1^2B_0^2) + \omega^2 E(A_1^2B_1^2) \\ & + \omega E(A_1^2B_2^2) + E(A_2^2B_0^2) + \omega E(A_2^2B_1^2) + \omega^2 E(A_2^2B_2^2)\ ]\end{aligned}$$

$$\begin{aligned}\mathrm{T}_2 = &(-\omega+7)E(A_0B_0) + (\omega^2+2)E(A_0B_1) + (-\omega+1)E(A_0B_2)\\ &+ (-\omega+1)E(A_1B_0) - (2\omega^2+1)E(A_1B_1) + (2\omega+1)E(A_1B_2)\\ &+ (\omega^2+2)E(A_2B_0) + (\omega-\omega^2)E(A_2B_1) - (2\omega^2+1)E(A_2B_2)\end{aligned}$$

$$\begin{aligned}\mathrm{T}_3 = &(-\omega+4)E(A_0B_0) + (\omega^2-1)E(A_0B_1) - (\omega+2)E(A_0B_2)\\ &- (\omega+2)E(A_1B_0) + (\omega^2+2)E(A_1B_1) + (5\omega+4)E(A_1B_2)\\ &+ (\omega^2-1)E(A_2B_0) + (\omega-4\omega^2)E(A_2B_1) + (\omega^2+2)E(A_2B_2)\end{aligned}$$

Or, on remarque que ces polynômes homogènes vérifient :

$$\begin{aligned}\mathrm{T}_2 - \mathrm{T}_3 = 3\,[\; &E(A_0B_0) + E(A_0B_0^2B_2^2) + E(A_0B_2) + E(A_1B_0) + \omega E(A_1B_0^2B_2^2)\\ &+ \omega^2 E(A_1B_2) + E(A_0^2A_1^2B_0) + \omega^2 E(A_0^2A_1^2B_0^2B_2^2) + \omega E(A_0^2A_1^2B_2)\;]\\ &= \text{c.c (conjugué complexe de } \mathrm{T}_1)\end{aligned}$$

et qu'on a également la propriété suivante :

$$\mathrm{Re}(\mathrm{T}_1 + \mathrm{T}_2 - \mathrm{T}_3) = \mathrm{Re}(\mathrm{T}_1 + \text{c.c}) = \mathrm{T}_1 + \text{c.c.} \tag{3.12}$$

D'après (3.12), on obtient :

$$\big(-9 \leqslant \mathrm{Re}(\mathrm{T}_1+\mathrm{T}_2) \leqslant 18 \quad \text{et} \quad -9 \leqslant \mathrm{Re}(-\mathrm{T}_3) \leqslant \frac{9}{2}\big) \;\Rightarrow\; -18 \leqslant \mathrm{T}_1 + \text{c.c} \leqslant \frac{45}{2}. \tag{3.13}$$

De plus, nous avons également :

$$\mathrm{T}_1 + \text{c.c} = 6\mathrm{B}_{\mathrm{Ji}} = 162\mathrm{B}_{\mathrm{Liang}} - 54 \tag{3.14}$$

D'après (3.9), (3.10), (3.11), (3.13) et (3.14), l'ajout des contraintes de multiplicité (3.8) nous permet d'obtenir deux nouvelles inégalités avec de meilleures bornes classiques que les inégalités (3.1) et (3.5) :

$$-3 \leqslant \mathrm{B}_{\mathrm{Ji}} \leqslant \frac{15}{4} \tag{3.15}$$

et

$$\frac{2}{9} \leqslant \mathrm{B}_{\mathrm{Liang}} \leqslant \frac{17}{36} \tag{3.16}$$

Comme ces inégalités atteignent la même valeur quatique maximale que précédemment pour les paramètres choisis, ces nouvelles bornes classiques (3.15) et (3.16) résultent en des violations plus hautes :

$$v_{\mathrm{Ji}} \simeq 5.117 \times \frac{4}{15} \simeq 1.364 \tag{3.17}$$

$$v_{\mathrm{Liang}} \simeq 0.7124 \times \frac{36}{17} \simeq 1.509 \tag{3.18}$$

Il est intéressant de remarquer qu'avec les trois bases sans biais, l'état $|\psi\rangle$ est optimal pour l'inégalité (3.9) mais pas pour les inégalités (3.10) et (3.11). Nous supposons que cet état permet d'atteindre le meilleur compromis lorsqu'on considère la valeur quantique des inégalités correspondant aux trois polynômes homogènes $\mathrm{T}_1, \mathrm{T}_2$ et $-\mathrm{T}_3$, ce qui le rend optimal pour l'inégalité (3.1).

3.2 Borne supérieure sur la violation des inégalités de Bell homogènes

Nous allons maintenant utiliser les propriétés de la norme matricielle présentées dans le Chapitre 1 pour dériver une borne supérieure sur la valeur de violation maximale des inégalités de Bell homogènes en dimension d à n parties.

Dans ce qui suit, nous utiliserons le théorème de Parseval pour la Transformée de Fourier Discrète en dimension d pour n parties décrit en (1.2). Grâce à ce théorème et aux propriétés de la norme matricielle, nous calculons la borne supérieure sur la valeur quantique d'un opérateur de Bell homogène Q_f décrit en (2.8).

Théorème 4
Soit Q_f un opérateur de Bell homogène en dimension d pour n parties et $Q_{fBell} = \frac{\rho}{d^n cos(\frac{\pi}{d})} Re(Q_f)$ avec $\rho = \mathrm{e}^{\frac{i\pi}{d}}$.

$$\left| \frac{\langle\psi| Q_{fBell} |\psi\rangle}{\langle\psi|\psi\rangle} \right| \leqslant \frac{d^{\frac{n}{2}}}{cos(\frac{\pi}{d})\sqrt{2}}. \tag{3.19}$$

Démonstration
Bien que la matrice Q_f ne corresponde pas à un opérateur normal, nous pouvons construire un opérateur normal (et en particulier hermitien) en considérant la matrice $\frac{1}{2}(Q_f + Q_f^\dagger)$.

Ainsi, nous avons :

$$\begin{aligned}\left| \frac{\langle\psi| Q_f + Q_f^\dagger |\psi\rangle}{\langle\psi|\psi\rangle} \right| &\leqslant \rho(Q_f + Q_f^\dagger) \leqslant \|Q_f + Q_f^\dagger\|_F \text{ (d'après Proposition 2)} \\ &= \sqrt{2}\|Q_f\|_F \text{ (car } Q_f \text{ et } Q_f^\dagger \text{ sont orthogonales d'après la Proposition 5).}\end{aligned}$$

On a également :

$$\begin{aligned}\|Q_f\|_F^2 &= \sum_{r\in\mathbb{Z}_d^n} |\widehat{f}(r)| \left\| \bigotimes_{i=1}^{n} X_i^{d-1-r_i} Z^{r_i} \right\|_F^2 \text{ (par orthogonalité d'après Proposition 5)} \\ &= \sum_{r\in\mathbb{Z}_d^n} |\widehat{f}(r)| d^n = d^{2n} \sum_{r\in\mathbb{Z}_d^n} |f(s)| \text{ (par l'égalité de Parseval en 1.2)} \\ &= d^{3n}.\end{aligned}$$

Finalement, on obtient :

$$\left|\mathrm{Re}\frac{\langle\psi| Q_f |\psi\rangle}{\langle\psi|\psi\rangle}\right| = \frac{1}{2}\left|\frac{\langle\psi| Q_f + Q_f^\dagger |\psi\rangle}{\langle\psi|\psi\rangle}\right| \leqslant \frac{1}{\sqrt{2}} d^{\frac{3n}{2}}. \tag{3.20}$$

Soit $Q_{fBell} = \frac{\rho}{d^n \cos(\frac{\pi}{d})}\mathrm{Re}(Q_f)$. Comme ρ vérifie $|\rho| = \left|\mathrm{e}^{\frac{i\pi}{d}}\right| = 1$, on a :

$$\left|\frac{\langle\psi| Q_{fBell} |\psi\rangle}{\langle\psi|\psi\rangle}\right| \leqslant \frac{d^{\frac{n}{2}}}{\cos(\frac{\pi}{d})\sqrt{2}}. \tag{3.21}$$

□

3.2.1 Résultats pour $n = 2$ et $d \leqslant 10$

Afin d'illustrer notre propos, nous allons calculer explicitement les bornes supérieures obtenues selon quelques valeurs de n et d. En posant $n = 2$, on obtient :

$$\left|\frac{\langle\psi| Q_{fBell} |\psi\rangle}{\langle\psi|\psi\rangle}\right| \leqslant \frac{d}{\cos(\frac{\pi}{d})\sqrt{2}} \tag{3.22}$$

Les bornes supérieures sur Q_{fBell} pour $n = 2$ et $d = 3, .., 10$ sont résumées dans le tableau ci-dessous :

d	3	4	5	6	7	8	9	10
Borne supérieure	$3\sqrt{2} \simeq 4.243$	4	4.370	4.899	5.494	6.123	6.772	7.435

Conclusion :

Dans ce chapitre, nous avons utilisé une particularité des mesures choisies par Ji *et al.* dans [41] puis Liang *et al.* dans [42] pour établir un lien entre leurs inégalité en dimension 3 pour deux parties à trois mesures par partie et les inégalités de Bell homogènes en dimension 3 pour deux parties à deux mesures par partie. Cette réécriture de leurs inégalités nous a permis de recalculer leurs bornes classiques et d'obtenir de meilleures valeurs de violation.

Nous avons également dérivé une borne supérieure sur les valeurs de violation des inégalités de Bell homogènes en dimension d pour n parties en utilisant le théorème de Parseval en dimension d pour n parties et les propriétés de la norme matricielle décrites dans le Chapitre 1.

Chapitre 4 :

Applications cryptographiques des inégalités de Bell homogènes

En cryptographie quantique, les protocoles de Distribution Quantique de Clés et de Partage de Secret Quantique intriqués exploitent le phénomène d'intrication pour établir de manière sûre un secret entre plusieurs participants. Cette propriété peut en effet servir de témoin au bon déroulement du protocole en permettant aux participants de détecter une perturbation grâce au calcul de la violation d'une inégalité de Bell bien choisie.

Dans la première partie de ce chapitre, nous commencerons par présenter les différents protocoles de Distribution Quantique de Clés pour deux parties en dimension d. Grâce à notre caractérisation de la mesure du produit d'observables en dimension d décrite dans le Chapitre 1, nous utiliserons les inégalités de Bell homogènes pour dériver de nouveaux protocoles de Distribution Quantique de Clés avec une meilleure résistance au bruit pour une sécurité équivalente contre la famille d'attaques individuelles par clonage optimal.

Dans la seconde partie, nous nous intéresserons aux protocoles de Partage de Secret en dimension d qui généralisent l'échange de clés entre deux parties au partage d'un secret entre n parties. Nous décrirons un nouveau protocole de Partage de Secret utilisant les ditters comme instruments de mesure et basé sur les notions de mesures accordées et mesures quasi-accordées, dont nous donnerons une définition. En posant $n = 2$, nous proposerons finalement un nouveau type de protocole de Distribution Quantique de Clés, différent de notre protocole h3DEB, qui exploite à la fois les inégalités de Bell homogènes et nos nouvelles notions de mesures accordées et quasi-accordées.

4.1 Distribution Quantique de Clés avec des qudits

Dans le second chapitre, nous avons présenté plusieurs protocoles de Distribution Quantique de Clés utilisant des qubits, dont le protocole à intrication Ekert91 souvent abrégé en E91.

Dans cette section, nous décrivons la variante de ce protocole E91 en dimensions supérieures : le protocole NDEB pour qudits décrit par Durt *et al* dans [28]. Nous présentons ensuite notre nouveau protocole hdDEB pour qudits décrit dans [3], qui exploite le facteur de violation élevé des inégalités de Bell homogènes pour obtenir une meilleure résistance au bruit tout en gardant un même niveau de sécurité que NDEB contre les attaques individuelles par clonage.

4.1.1 Le protocole NDEB pour qudits

Dans ce qui suit, nous décrivons le protocole NDEB introduit par Durt *et al* dans [28] et qui généralise le protocole E91 à la dimension d.

Le protocole NDEB utilises des inégalités en dimension d introduites dans [33], où elles sont désignées par le terme de *CHSH généralisées* mais auxquelles nous ferons référence dans cette thèse comme les *inégalités CGLMP-d* déjà décrites en (2.4). L'un des états maximalement intriqués, décrit en (1.10), et les quatres bases en dimension d décrites en (2.1) permettent d'obtenir des violations de ces inégalités.

Dans la description du protocole NDEB qui suit, on donne une description des ditters permettant de mesurer les observables qui correspondent à ces quatre bases.

Déroulement du protocole NDEB et bases utilisées :

Alice dispose de quatre observables A_a avec $a = 0$ à 3 correspondant aux bases décrites en (2.1), c'est-à-dire aux mesures effectuées par des ditters de déphasages $(1, \theta^a, \theta^{2a}, ..., \theta^{(d-1)a})$.

Bob dispose des quatre observables B_b avec $b = 0$ à 3 correspondant aux bases décrites en (2.1), c'est-à-dire aux mesures effectuées par les ditters de déphasages $(1, \theta^{-b}, \theta^{-2b}, ..., \theta^{-(d-1)b})$.

Procédure :

1. Alice et Bob obtiennent des paires de qudits intriqués dans un état maximalement intriqué décrit en (1.10).
2. Pour chacun de ces états, Alice tire au hasard un $a \in \{0, 1, 2, 3\}$ et effectue la mesure correspondant à l'observable A_a tandis que Bob fait de même pour un $b \in \{0, 1, 2, 3\}$ et pour l'observable B_b.
3. Lorsque $a = b$, les résultats obtenus sont parfaitement corrélés. En effet, les deux ditters utilisés par Alice et Bob effectuent sur l'état maximalement intriqué la transformation $(H \otimes H)(D_\Theta \otimes D_{\Theta^*})$ avec $\Theta = (1, \theta^a, \theta^{2a}, ..., \theta^{(d-1)a})$. On vérifie plus bas que :
$$(H \otimes H)(D_\Theta \otimes D_{\Theta^*})(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle) = \frac{1}{\sqrt{d}} \sum_{\substack{k,k'=0 \\ k+k' \equiv 0[d]}}^{d-1} |kk'\rangle. \tag{4.1}$$
En conséquence, lorsque $a = b$, Alice et Bob obtiennent un dit pour la clé partagée.

Proposition 8
Soit $|\psi_{GHZ_2}\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle$ *un état maximalement intriqué en dimension* d.

Supposons qu'Alice et Bob disposent de deux ditters qui effectuent sur l'état $|\psi_{GHZ_2}\rangle$ *la transformation* $(H \otimes H)(D_\Theta \otimes D_{\Theta'})$, *avec* $\Theta = (\theta_0, \theta_1, ..., \theta_{(d-1)})$ *et* $\Theta' = (\theta'_0, \theta'_1, ..., \theta'_{(d-1)})$.

Si pour tout $k = 0, ..., d-1$ *les phases vérifient* $\theta'_k = \theta^*_k$, *Alice et Bob obtiennent des résultats parfaitement corrélés.*

DÉMONSTRATION
Soit $|\psi_{\mathrm{GHZ}_2}\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle$ un état maximalement intriqué en dimension d.

Alice et Bob disposent de deux ditters qui effectuent sur l'état $|\psi_{\mathrm{GHZ}_2}\rangle$ la transformation $(H \otimes H)(D_\Theta \otimes D_{\Theta'})$, avec $\Theta = (\theta_0, \theta_1, ..., \theta_{(d-1)})$ et $\Theta' = (\theta'_0, \theta'_1, ..., \theta'_{(d-1)})$.

On écrit alors :

$$\begin{aligned}(H \otimes H)(D_\Theta \otimes D_{\Theta'}) &= (HD_\Theta \otimes HD_{\Theta'}) \\ &= \frac{1}{d}\Big(\sum_{k,l=0}^{d-1} \omega^{kl}\theta_l \,|k\rangle\langle l| \otimes \sum_{k',l'=0}^{d-1} \omega^{k'l'}\theta'_{l'} \,|k'\rangle\langle l'| \Big) \\ &= \frac{1}{d}\Big(\sum_{k,l,k',l'=0}^{d-1} \omega^{kl+k'l'}\theta_l\theta'_{l'} \,|kk'\rangle\langle ll'| \Big)\end{aligned}$$

En appliquant cette transformation sur l'état $|\psi_{\mathrm{GHZ}_2}\rangle$, on obtient :

$$(HD_\Theta \otimes HD_{\Theta'})\Big(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle\Big) = \frac{1}{d\sqrt{d}}\Big(\sum_{j=0}^{d-1} \sum_{k,k'=0}^{d-1} \omega^{j(k+k')}\theta_j\theta'_j \,|kk'\rangle\Big)$$

Or, pour un u fixé, on a :

$$\sum_{j=0}^{d-1} \omega^{ju} = \begin{cases} d & \text{si } u \equiv 0 \pmod d \\ 0 & \text{sinon.} \end{cases}$$

En posant $u = k + k'$, on réécrit donc :

$$(HD_\Theta \otimes HD_{\Theta'})\Big(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle\Big) = \frac{1}{\sqrt{d}}\Big(\sum_{j=0}^{d-1} \theta_j\theta'_j\Big)\Big(\sum_{\substack{k,k'=0 \\ k+k' \equiv 0 \pmod d}}^{d-1} |kk'\rangle\Big)$$

De plus, si $\theta'_j = \theta^*_j$ pour tout $j = 0, ..., d-1$, on obtient le résultat :

$$(HD_\Theta \otimes HD_{\Theta'})\Big(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle\Big) = \frac{1}{\sqrt{d}}\Big(\sum_{\substack{k,k'=0 \\ k+k' \equiv 0[d]}}^{d-1} |kk'\rangle\Big).$$

□

4.1.1.1 Sécurité du protocole NDEB

Lorsque leurs choix de bases vérifient $a \neq b$, Alice et Bob peuvent utiliser une partie de leurs résultats pour calculer deux violations de l'inégalité CGLMP-d en dimension d décrite en (2.4).

Si les deux valeurs de violations dépassent 1, ils peuvent utiliser la clé secrète partagée sans risque. Dans le cas contraire, leurs bits de clé secrète sont potentiellement compromis et donc inutilisables. Le protocole doit alors être recommencé du début.

Pour la configuration 1 (resp. 2), l'inégalité CGLMP-d s'exprime avec le polynôme T_1 (resp. T_2) suivant :

$$T_1 = A_0B_1 + A_0B_3 + A_2B_1 - A_2B_3 \quad (\text{resp.} \quad T_2 = A_1B_0 + A_1B_2 + A_3B_0 - A_3B_2).$$

Les choix de bases et l'état décrits plus haut permettent d'obtenir deux violations de l'inégalité CGLMP-d avec T_1 et T_2.

Comme expliqué dans le Chapitre 2, choisir une inégalité tolérant un seuil de bruit supérieur au bruit minimal généré par une attaque signifie qu'on ne sera pas en mesure de détecter cette attaque. Il est donc important de choisir une inégalité permettant la meilleure résistance au bruit possible tout en restant sous le seuil maximal toléré par cette attaque, dans notre cas l'attaque par clonage optimal.

Les valeurs de violation de CGLMP-d obtenues pour $d = 3, 4, 5$ sont décrites dans le tableau suivant :

d	$v_{\text{CGLMP}-d}$
3	1.436
4	1.448
5	1.455

Tableau 4.1 – Valeurs de violation de l'inégalité CGLMP-d pour $d = 3, 4, 5$

Dans les cas $d = 3, 4, 5$ les valeurs de violations de de CGLMP-d sont toutes sous le seuil de sécurité décrit dans le tableau (2.2), ce qui garantit la sécurité du protocole NDEB contre les attaques individuelles par clonages.

Résumé du protocole NDEB :

Les différents choix de bases du protocole NDEB peuvent se résumer dans le tableau suivant, qui est le même que celui du protocole E91 :

	B_0	B_1	B_2	B_3
A_0	k	c_1		c_1
A_1	c_2	k	c_2	
A_2		c_1	k	c_1
A_3	c_2		c_2	k

k : Alice et Bob obtiennent des dits de clé.

c_1 et c_2 : Alice et Bob obtiennent des valeurs pour vérifier la violation de CGLMP-d.

Tableau 4.2 – Résumé du protocole NDEB

Ainsi, sur les $4 \times 4 = 16$ choix de mesures possibles, on a :

- 4 choix résultant en un dit de clé (**25**%),
- 8 choix intervenant dans la vérification des inégalités CGLMP-d (**50**%),
- 4 choix inutilisés (**25**%).

Exemple pour $d = 3$: le protocole 3DEB

Le protocole 3DEB utilise l'inégalité de Bell pour qutrits nommée CHSH-3 décrite par Durt *et al.*. dans [43] et que nous rappelons en (2.5).

Les quatre bases optimales [29, 30, 31] permettant d'obtenir la violation maximale de l'inégalité CHSH-3 sont décrites dans la Figure 2.1. Ces bases et un état maximalement intriqué décrit en (1.10) permettent d'obtenir le facteur de violation $v_{\text{CHSH}-3} = (6 + 4\sqrt{3})/9 \simeq 1.436$.

4.1.2 Notre protocole hdDEB pour qudits

Nous allons maintenant présenter notre nouveau protocole hdDEB qui utilise des inégalités de Bell homogènes en dimension d appelées hCHSH-d au lieu des inégalités CGLMP-d.

Bases et état utilisés dans le protocole hdDEB

Tout comme dans le protocole NDEB décrit précédemment, nous utilisons l'état maximalement intriqué $|\psi_{\text{GHZ}_2}\rangle$ décrit en (1.10) et les bases décrites en (2.1). Nous notons A_a avec $a = 0, .., d-1$ l'observable paramétrée par un déphasage $(1, \theta^a, .., \theta^{(d-1)a})$, et B_b avec $b = 0, .., d-1$ l'observable paramétrée par $(1, \theta^{-b}, \theta^{-(d-1)b})$.

Bien que l'inégalité de Bell homogène hCHSH-d fasse intervenir des mesures de produits d'observables, chaque mesure s'implémente avec un ditter d'après la Proposition 7.

Procédure :

1. Alice et Bob obtiennent des paires de qudits intriqués dans un état intriqué $|\psi_d\rangle$.
2. Pour chacun de ces états, Alice tire au hasard un $a \in \{0, 1, 2, 3\}$ et effectue la mesure correspondant à l'observable A_a tandis que Bob fait de même pour un $b \in \{0, 1, 2, 3\}$ et pour l'observable B_b.
3. Lorsque $a = b$, leurs résultats sont parfaitement corrélés d'après la Proposition 8.

Exemple pour $d = 3$: le protocole h3DEB

Notre étude détaillée du cas $d = 3$ a fait l'objet d'une publication dans la revue internationale *Quantum Information and Computation* [44]. Le protocole h3DEB utilise l'inégalité de Bell homogène pour qutrits nommée hCHSH-3, qu'on écrit :

$$-\frac{2}{9}\mathrm{Re}(T_3) \leqslant 1 \tag{4.2}$$

pour le polynôme T_3 décrit précédemment. Les différents choix de bases du protocole h3DEB peuvent se résumer dans le tableau suivant :

	B_0^2	B_0B_2	B_2^2	B_1^2	B_1B_3	B_3^2
A_0^2	k			c_1	c_1	c_1
A_0A_2		k		c_1	c_1	c_1
A_2^2			k	c_1	c_1	c_1
A_1^2	c_2	c_2	c_2	k		
A_1A_3	c_2	c_2	c_2		k	
A_3^2	c_2	c_2	c_2			k

k : Alice et Bob obtiennent des dits de clé.

c_1 et c_2 : Alice et Bob obtiennent des valeurs pour vérifier la violation de hCHSH-3.

Tableau 4.3 – Résumé du protocole h3DEB

Ainsi, sur les $6 \times 6 = 36$ choix de mesures possibles, on a :

- 6 choix résultant en un trit de clé ($\mathbf{16,67}\%$),
- 18 choix intervenant dans la vérification d'une inégalité hCHSH-3 ($\mathbf{50}\%$),
- 12 choix inutilisés ($\mathbf{33,33}\%$).

4.1.2.1 Sécurité du protocole hdDEB

Comme expliqué dans le Chapitre 2 et rappelé dans la section sur la sécurité du protocole NDEB, on est assuré de détecter une attaque grâce à la vérification d'une inégalité de Bell si le seuil de bruit maximum toléré par l'inégalité est inférieur au seuil de bruit minimum provoqué par l'attaque. On se place ici dans le cadre d'une attaque par clonage optimal dont les seuils de bruit minimum sont décrits dans le tableau (2.2).

Choix des paramètres et violation de hCHSH-d :

Montrons d'abord que le cloneur décrit par Durt *et al.* en [28] est également optimal pour notre procotole.

Proposition 9

Les $2d$ bases considérées dans notre protocole sont copiées avec une fidélité maximale lorsqu'on utilise le cloneur optimal décrit par Durt et al. dans [28].

Démonstration

Quatre de nos bases sont les bases décrites en (2.1) et déjà utilisées dans le protocole NDEB. Les $2(d-2)$ bases restantes ont des vecteurs de la forme :

$$\tfrac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i\gamma_j} |j\rangle.$$

Mais le cloneur décrit par Durt *et al.* en [28] est optimal pour tous les états de la forme :

$$\sum_{j=0}^{d-1} \xi_j |jj\rangle \text{ pour tout } \delta_j \text{ vérifiant } |\xi_j|^2 = \tfrac{1}{d}.$$

En conséquence, ce cloneur est également optimal pour nos $2(d-2)$ bases restantes. □

On considère les états $|\psi_{\mathrm{GHZ}_2}\rangle$ pour $d = 3, 4, 5$ et on utilise les inégalités de Bell homogènes associées à chacun de ces états :

$$\frac{1}{d^2 \cos(\frac{\pi}{d})} \mathrm{Re}(\rho E(T_d)) \leqslant 1 \tag{4.3}$$

avec les polynôme homogène T_d correspondants qu'on liste ci-dessous :

$$\begin{aligned} T_3 = -\big[&(\omega-4)(A_0^2B_1^2) + (\omega+2)(A_0^2B_1B_3) + (\omega-1)(A_0^2B_3^2) \\ &+ (\omega+5)(A_0A_2B_1^2) + (\omega+2)(A_0A_2B_1B_3) + (\omega+1)(A_0A_2B_3^2) \\ &+ (\omega+5)(A_2^2B_1^2) + (\omega+2)(A_2^2B_1B_3) + (\omega-1)(A_2^2B_3^2)\big], \end{aligned}$$

$$\begin{aligned} T_4 = &-(3\omega+1)(A_0^3B_1^3) - (\omega+1)(A_0^3B_1^2B_3) - 5(\omega-1)(A_0^3B_1B_3^2) \\ &- (3\omega-1)(A_0^3B_3^3) + (\omega+1)(A_0^2A_2B_1^3) - (\omega+3)(A_0^2A_2B_1^2B_3) \\ &- (\omega+1)(A_0^2A_2B_1B_3^2) - (3\omega+1)(A_0^2A_2B_3^3) + (3\omega+1)(A_0A_2^2B_1^3) \\ &+ (5\omega+1)(A_0A_2^2B_1^2B_3) - (7\omega+1)(A_0A_2^2B_1B_3^2) + 3(\omega+1)(A_0A_2^2B_3^3) \\ &- 5(\omega+1)(A_2^3B_1^3) + (\omega-1)(A_2^3B_1^2B_3) + (\omega+1)(A_2^3B_1B_3^2) \\ &- (\omega-1)(A_2^3B_3^3), \end{aligned}$$

$$\begin{aligned} T_5 = &(-5\omega^3-2\omega^2-4\omega+1)A_0^4B_1^4 + (4\omega^3-\omega^2+2\omega)A_0^4B_1^3B_3 + (\omega^3+2\omega^2+\omega-2)A_0^4B_1^2B_3^2 \\ &+ (-3\omega^2+3\omega)A_0^4B_1B_3^3 + (-8\omega^3-6\omega^2-7\omega+1)A_0^4B_3^4 + (\omega^3+5\omega^2+4\omega)A_0^3A_2B_1^4 \\ &+ (-2\omega^3-3\omega^2-6\omega+1)A_0^3A_2B_1^3B_3 + (\omega^3+\omega^2+2\omega+1)A_0^3A_2B_1^2B_3^2 \\ &+ (2\omega^2-2\omega+5)A_0^3A_2B_1B_3^3 + (-5\omega^2-3\omega-2)A_0^3A_2B_3^4 + (-3\omega^3+2\omega^2-3\omega-1)A_0^2A_2^2B_1^4 \\ &+ (-3\omega^3-4\omega-3)A_0^2A_2^2B_1^3B_3 + (-7\omega^3-10\omega^2-2\omega-6)A_0^2A_2^2B_1^2B_3^2 \\ &+ (-3\omega^2+3\omega)A_0^2A_2^2B_1B_3^3 + (-2\omega^3-4\omega^2+\omega-5)A_0^2A_2^2B_3^4 + (3\omega^3+4\omega^2-2)A_0A_2^3B_1^4 \end{aligned}$$

$$+(-4\omega^3-2\omega^2-2\omega-2)A_0A_2^3B_1^3B_3+(\omega^2-\omega-3)A_0A_2^3B_1^2B_3^2+(-3\omega^2-2\omega)A_0A_2^3B_1B_3^3$$
$$+(-4\omega^3-3\omega^2-3)A_0A_2^3B_3^4+(4\omega^3+\omega^2-2\omega-3)A_2^4B_1^4+(\omega^2-1)A_2^4B_1^3B_3$$
$$+(2\omega^3-2\omega^2)A_2^4B_1^2B_3^2+(2\omega^2-2\omega)A_2^4B_1B_3^3+(\omega^3+3\omega^2-\omega-1)A_2^4B_3^4.$$

Chaque choix de polynôme homogène est résumé dans le tableau suivant :

d	T_d	$v_{\text{hCHSH}-d}$
3	T_3	1.505
4	T_4	1.546
5	T_5	1.545

Tableau 4.4 – Valeurs de violation de l'inégalité hCHSH-d pour l'état $|\psi_{\text{GHZ}_2}\rangle$ en fonction du polynôme homogène T_d

Dans les cas $d = 3, 4, 5$ les valeurs de violations de de hCHSH-d obtenues plus haut sont effectivement toutes sous le seuil de sécurité décrit dans le tableau (2.2), ce qui garantit la sécurité du protocole hdDEB contre les attaques individuelles par clonage.

4.1.3 Comparaison entre NDEB et hdDEB et sécurité contre les attaques individuelles par clonage

Maintenant que nous avons présenté les inégalités de Bell homogènes à utiliser dans nos protocoles pour $d = 3, 4, 5$ et leurs valeurs de violation associées pour les bases décrites en (2.1) et l'état $|\psi_{\text{GHZ}_2}\rangle$, nous pouvons comparer notre nouvelle famille de protocoles à la famille des protocoles NDEB.

En observant les résultats de violation de NDEB et hdDEB en fonction de d, on peut remarquer que pour chaque $d = 3, 4, 5$ les valeurs de violation de ces deux protocoles sont toutes inférieures au critère de sécurité du Tableau 2.2. Cela permet de conclure que les deux protocoles sont sûrs contre les attaques individuelles par clonage optimal.

On peut également remarquer que, pour chaque $d = 3, 4, 5$, il y a une grande différence entre les valeurs de violations atteignables par CGLMP-d et la valeur maximale tolérée par le seuil de sécurité. Cette différence peut se combler par l'utilisation de nos inégalités CGLMP-d qui atteignent de plus grandes valeurs de violation.

En effet, non seulement notre nouveau protocole tolère davantage de bruit dans le canal que NDEB pour une sécurité équivalente contre les attaques individuelles par clonage, mais il permet également de combler l'écart entre le seuil de sécurité et $v_{\text{CGLMP}-d}$.

Le tableau suivant permet de comparer les différentes valeurs de violation des protocoles NDEB et hdDEB avec le critère de sécurité pour $d = 3, 4, 5$:

d	$v_{\text{CGLMP}-d}$	$v_{\text{hCHSH}-d}$	Critère de sécurité
3	1.436	1.505	$v < 1.508$
4	1.448	1.546	$v < 1.549$
5	1.455	1.545	$v < 1.575$

Tableau 4.5 – Comparaison entre les valeurs de violation des inégalités CGLMP-d et hCHSH-d

4.2 Partage de Secret Quantique avec des qudits

En cryptographie quantique, les participants utilisent des clés secrètes partagées pour protéger leurs communications. Les protocoles de Partage de Secret Quantique (abrégés en QSS) permettent à n participants d'établir un secret qui ne peut être récupéré sans la coopération de tous. Chaque participant numéroté par $i = 1, ..., n$ disposera donc de son secret S_i, qui est une portion du secret total S, mais aucun d'entre eux ne connaît S. De plus, ils doivent tous collaborer pour utiliser le secret total S.

Exemple 8 Exemple de partage d'un secret S entre n participants :

$$S = S_1 \oplus S_2 \oplus ... \oplus S_n.$$

Certains de ces protocoles ont été testés expérimentalement, comme dans [45], [46] pour les protocoles à variables discrètes et [47], [48] pour les protocoles à variables continues.

Tout comme dans le cas de la Distribution Quantique de Clés entre deux participants, on peut différencier les protocoles sans intrication, comme dans [49] et [50], des protocoles dont la sécurité est basée sur l'intrication quantique. Les premiers protocoles à intrication avec des variables discrètes pour qubits et à 3 ou 4 participants, surnommés HBB et KKI, sont décrits par Hillery, Bužek, Berthiaume dans [51] et par Karlsson, Koashi, Imoto dans [52]. Yu, Lin et Huang généralisent les protocoles de type HBB à n participants et à des systèmes en dimension d dans [53].

Dans [54] et [55], Scarani *et al* établissent un lien entre la sécurité des protocoles intriqués pour qubits contre les attaques individuelles et la violation d'inégalités de Bell. Dans [56], Sen *et al* dérivent un critère de sécurité pour ces protocoles à n participants, toujours contre les attaques individuelles, en se basant sur la violation d'inégalités de Bell.

Dans la section précédente, nous avons expliqué comment partager des clés secrètes avec des systèmes en dimension d entre deux participants. Nous présentons maintenant un environnement général pour construire des protocoles de Partage de Secret Quantique pour systèmes en dimension d et pour n participants effectuant des mesures à l'aide de ditters.

Pour ce faire, nous nous sommes inspirés des protocoles décrits par Yu *et al.* dans [53]. Nous décrivons deux nouvelles notions de mesures *accordées* et *quasi-accordées* dont nous étudions quelques propriétés intéressantes. Dans le cadre de cette nouvelle description, nous réinterprétons également le protocole pour Bases Sans Biais (MUBs) décrits par Yu *et al.* dans [53] et nous construisons deux protocoles de Partage de Secret Quantique pour $d = 3$ avec $n = 2$ et $n = 3$ en se basant sur des mesures *accordées* et *quasi-accordées*.

Dans ce qui suit, nous utilisons l'état maximalement intriqué en dimension d pour n parties noté $|\psi_{\mathrm{GHZ}_n}\rangle$ et décrit en 1.9.

4.2.1 Mesures accordées et quasi-accordées

Afin de concevoir de nouveaux protocoles de Partage de Secret Quantique pour systèmes en dimension d, il faut dériver une ou plusieurs conditions qui, lorsqu'elles sont satisfaites, assurerons que les n participants qui coopèrent obtiennent un dit secret pour des choix de mesures spécifiques. En considérant les rares protocoles à intrication présents dans la littérature, nous avons réalisé que déterminer ces conditions est loin d'être immédiat et qu'elles sont souvent valides pour des bases de mesure très précises, comme le cas des Bases Sans Biais dans le protocole de Yu *et al* décrit en [53].

Grâce à l'introduction de deux nouvelles notions, les mesures *accordées* et *quasi-accordées*, nous construisons un environnement plus général permettant de dériver des conditions utilisables pour le Partage de Secret Quantique grâce au choix de bases de mesure appropriées qui permettrons de maximiser le taux de génération de dits secrets. Nous montrons également comment le protocole à intrication avec Bases Sans Biais de Yu *et al* dans [53] constitue un cas particulier de notre travail.

Pour $i = 1, .., n$, chaque participant i effectue une mesure avec le ditter paramétré par le d-uplet de déphasages $\Theta_{(i)} = (\theta_{(i),0}, ..., \theta_{(i),d-1})$ mesurant l'observable $Z_{\Theta_{(i)}}$.

Cette observable admet les vecteurs propres suivants :

$$B_{\Theta_{(i)}} = D_{\Theta^*_{(i)}} H^\dagger = \frac{1}{\sqrt{d}} \sum_{k,l=0}^{d-1} \theta^*_{(i),k} \omega^{-kl} |k\rangle \langle l| .$$

En conséquent, la base de mesure correspondant à la mesure totale effectuée par l'ensemble des participants s'écrit :

$$B_\Theta = \bigotimes_{i=1}^{n} B_{\Theta_{(i)}} = \frac{1}{d^{\frac{n}{2}}} \sum_{K,L \in \mathbb{Z}_d^n} \prod_{i=1}^{n} \theta^*_{(i),k_i} \omega^{-K.L} \left|K\right\rangle \left|L\right\rangle .$$

Cette mesure globale équivaut à la mesure suivante dans la base canonique $\mathbb{B}$:

$$\widetilde{\left|\psi\right\rangle} = B_\Theta^\dagger \left|\psi_{\mathrm{GHZ}_n}\right\rangle = \frac{1}{d^{\frac{n+1}{2}}} \sum_{L} (\sum_{k=0}^{d-1} \prod_{i=1}^{n} \theta_{(i),k} \omega^{k \sum l_i}) \left|L\right\rangle .$$

La probabilité d'obtenir l'issue L est $\frac{1}{d^{n-1}}$ si on choisit :

$$\sum_{i=1}^{n} l_i \equiv 0 \pmod d \quad \text{et} \quad \forall k = 0, ..., d-1 \quad \prod_{i=1}^{n} \theta_{(i),k} = 1 \tag{4.4}$$

et zéro sinon.

Avec cette condition sur les valeurs des déphasages $\theta_{(i),k}$ pour chaque i, on définit deux nouvelles notions qu'on utilisera ensuite dans des protocoles de Partage de Secret Quantique pour obtenir des dits aléatoires secrets.

Définition 51 : Mesures accordées

Soient n mesures décrites par les observables $A_1, ..., A_n$ correspondant aux n ditters de déphasages $\Theta_{(1)}, ..., \Theta_{(n)}$ avec $\Theta_{(i)} = (\theta_{(i),0}, \theta_{(i),1}, ..., \theta_{(i),d-1})$. Si ces mesures satisfont la condition (4.4), on les appelle *mesures accordées.*

Définition 52 : Mesures quasi-accordées

Pour tout $k = 0, ..., d-1$, le ditter paramétré par les déphasages $(\mu^k, ..., \mu^k)$ avec $\mu^d = 1$ mesure l'observable $\mu^* X$ d'après la Propriété 2 (a). Comme nous pouvons toujours compenser le nombre complexe μ^* en multipliant l'issue d'une des parties par μ, la définition de *mesures accordées* peut s'étendre à *mesures quasi-accordées* en remplaçant la condition (4.4) par :

$$\sum_{i=1}^{n} l_i \equiv 0 \pmod d \quad \text{et} \quad \forall k = 0, ..., d-1 \quad \prod_{i=1}^{n} \theta_{(i),k} = \mu^k \text{ avec } \mu^d = 1. \tag{4.5}$$

Pour tout $k = 0, ..., d-2$, les n mesures décrites par les observables $A_1, ..., A_n$ sont dites *quasi-accordées* si le nombre complexe $\mu = \prod_{i=1}^{n} \frac{\theta_{(i),k+1}}{\theta_{(i),k}}$ ne dépend pas de k et si il vérifie $\mu^d = 1$.

Proposition 10

Pour $i = 1, ..., n$, soient les mesures décrites par les observables A_i et correspondant aux ditters de déphasages respectifs $\Theta_{(i)}$. Soient également les mesures décrites par les observables B_i correspondant aux ditters de déphasages respectifs $\Lambda_{(i)}$.

a) Supposons que les n mesures A_i soient accordées et que les n mesures B_i soient elles aussi accordées. Dans ce cas, pour tout (u, v) vérifiant $u + v = d - 1$, les n mesures $A_i^u B_i^v$ sont également accordées.

b) Cette assertion reste vraie lorsqu'on considère des mesures quasi-accordées au lieu de mesures accordées.

Démonstration

Etant donné que (a) est un cas particulier de (b) pour lequel on considère $\mu = \mu' = 1$, nous démontrerons uniquement (b).

Supposons que les mesures A_i sont quasi-accordées et que les mesures B_i le sont également. D'après (4.5), on a donc que $\sum_{i=1}^{n} l_i \equiv 0 \pmod d$ et que, pour tout $k = 0, ..., d-1$, les mesures A_i et B_i vérifient :

$$\prod_{i=1}^{n} \theta_{(i),k} = \mu^k \quad \text{et} \quad \prod_{i=1}^{n} \lambda_{(i),k} = \mu'^k.$$

avec $\mu = \prod_{i=1}^{n} \frac{\theta_{(i),k+1}}{\theta_{(i),k}}$, $\mu' = \prod_{i=1}^{n} \frac{\lambda_{(i),k+1}}{\lambda_{(i),k}}$ et $\mu^d = \mu'^d = 1$.

Dans ce cas, les mesures $A_i^u B_i^v$ définies en (7) vérifient :

$$\begin{aligned}\prod_{i=1}^{n} \gamma_{(i),k} &= \prod_{i=1}^{n} \theta^*_{(i),k-u} \theta^*_{(i),k-u+1} ... \theta^*_{(i),k-1} \lambda^*_{(i),k+1} \lambda^*_{(i),k+2} ... \lambda^*_{(i),k+v} \\ &= \mu^{-(k-u)} \mu^{-(k-u+1)} .... \mu^{-(k-u+u-1)} \mu'^{-(k+1)} \mu'^{-(k+2)} ... \mu'^{-(k+v)} \\ &= \nu \quad \text{avec} \quad \nu = \prod_{i=1}^{n} \frac{\gamma_{(i),k+1}}{\gamma_{(i),k}} \quad \text{et} \quad \nu^d = 1.\end{aligned}$$

□

4.2.2 Réinterprétation du protocole de Partage de Secret Quantique avec des bases sans biais de Yu *et al.*

Pour tout d puissance impaire d'un nombre premier, considérons les matrices de Pauli généralisées en dimension d décrites en (1.4). Les observables mesurant les d MUBs utilisées par Yu *et al.* dans leur protocole de Partage de Secret Quantique en [53] peuvent s'exprimer grâce aux matrices XZ^j pour $j = 1, ..., d$ décrites en (1.6).

D'après la proposition 6, nous savons que les observables correspondant aux d MUBs de matrices XZ^j pour $j = 1, ..., d$ peuvent se mesurer avec les ditters de déphasages :

$$\forall k = 1, ..., d-1 \quad \theta_k = \omega^{-j\frac{k(k-1)}{2}}.$$

Considérons n participants qui utilisent d MUBs d'observables $X, XZ, XZ^2, ..., XZ^{d-1}$. On numérote par j_i la mesure effectuée par la partie i et qui correspond à l'observable XZ^{j_i}. On va montrer que notre notion de mesures accordées résulte en la même condition que celle décrite par Yu *et al.* dans [53] en réécrivent le produit des déphasages comme suit :

$$\forall k = 0, ..., d-1 \qquad \prod_{i=1}^{n} \omega^{-j_i\frac{k(k-1)}{2}} = \omega^{-(\sum_{i=1}^{n} j_i)\frac{k(k-1)}{2}} = 1.$$

Pour vérifier cette condition pour n'importe quelle valeur de k, et donc en particulier pour $k = 2$ qui donne $\frac{k(k-1)}{2} = 1$, les j_i doivent vérifier la même condition que celle décrite par Yu *et al.* dans [53] :

$$\sum_{i=1}^{n} j_i \equiv 0 \pmod{d}.$$

En conséquent, on peut réinterpréter le protocole de Partage de Secret Quantique de Yu *et al.* en [53] en fonction de notre notion nouvellement définie de mesures accordées, ce qui nous permet d'obtenir exactement la même condition pour établir le secret.

4.2.3 Ditters paramétrés par des puissances successives

Dans le reste de ce chapitre, nous utiliserons une famille particulière de ditters paramétrés par des déphasages de la forme $\theta_k = \zeta^k$ pour $k = 0, .., d-1$ et $\zeta = \mathrm{e}^{\frac{2i\pi}{gd}}$ un complexe avec $g \in \mathbb{N}^*$. Chaque participant est numéroté par $i = 0, ..., n$ et mesures des observables de la forme $Z_{\Theta_{(i),p}}$ qui correspondent aux ditters paramétrés par les triplets de déphasages :

$$\Theta_{(i),p} = (1, \zeta^p, \zeta^{2p}, ..., \zeta^{(d-1)p}) \qquad \text{pour} \qquad p = 0, ..., d-1.$$

Théorème 5
Soit $\zeta = \mathrm{e}^{\frac{2i\pi}{gd}}$ un complexe avec $g \in \mathbb{N}^*$.

Notons A_{a_i} (resp. B_{b_i}) l'observable du participant i qui correspond à la mesure effectuée par le triplet de déphasages $\Theta_{(i),a_i} = (\theta_{(i),0}, ..., \theta_{(i),d-1})$ avec $\theta_{(i),k} = \zeta^{a_i k}$ (resp. $\Lambda_{(i),b_i} = (\lambda_{(i),0}, ..., \lambda_{(i),d-1})$ avec $\lambda_{(i),k} = \zeta^{b_i k}$).

Alors, pour tout (u, v) vérifiant $u + v = d - 1$, les mesures correspondant aux observables $A_{a_i}^u B_{b_i}^v$ sont quasi-accordées si et seulement si elles vérifient :

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \equiv 0 \pmod{g}.$$

Démonstration
L'observable $A_{a_i}^u B_{b_i}^v$ est mesurée par un ditter paramétré par les déphasages suivants :

$$\forall k = 0, .., d-1 \quad \sigma_{(i),k} = \zeta^{-a_i([k-u]_d + ... + [k-1]_d) - b_i([k+1]_d + ... + [k+v]_d)}.$$

En posant $a = \sum_{i=1}^{n} a_i$ et $b = \sum_{i=1}^{n} b_i$, les produits des phases s'écrivent :

$$\forall k = 0, .., d-1 \quad \sigma_k := \prod_{i=1}^{n} \sigma_{(i),k} = \zeta^{-a([k-u]_d + ... + [k-1]_d) - b([k+1]_d + ... + [k+v]_d)}.$$

Pour $1 \leqslant t \leqslant u$, on a $[k+1-t]_d - [k-t]_d = 1$ sauf lorsque $t \equiv k+1 \pmod{d}$, auquel cas on obtient $d-1$. De même pour $1 \leqslant t \leqslant u$, on a $[k+1+t]_d - [k+t]_d = 1$ sauf lorsque $t \equiv -(k+1) \pmod{d}$, auquel cas on obtient également $d-1$. On en déduit :

$$\frac{\sigma_{k+1}}{\sigma_k} = \begin{cases} \zeta^{-au-bv+ad} & \text{pour } k = 0, ..., u-1 \\ \zeta^{-au-bv} & \text{pour } k = u \\ \zeta^{-au-bv+bd} & \text{pour } k = u+1, ..., d-1 \end{cases}$$

D'après la définition 52, les mesures correspondant aux observables $A_{a_i}^u B_{b_i}^v$ sont quasi-accordées si et seulement si elles vérifient, pour tout $k = 0, .., d-2$, les conditions $\zeta^{ad} = \zeta^{bd} = 1$ et $\zeta^{-(au+bv)} = \mu$ pour $\mu^d = 1$.

Comme $\zeta^{gd} = 1$, on a la première condition $\zeta^{ad} = \zeta^{bd} = 1$ si et seulement si $ad \equiv bd \equiv 0 \pmod{gd}$, c'est-à-dire $a \equiv b \equiv 0 \pmod{g}$. De plus, $a \equiv b \equiv 0 \pmod{g}$ implique $au + bv \equiv 0 \pmod{g}$, ce qui assure la deuxième condition $\zeta^{-(au+bv)} = \mu$ pour $\mu^d = 1$.

Les mesures correspondant aux observables $A_{a_i}^u B_{b_i}^v$ sont donc quasi-accordées si et seulement si elles vérifient $a \equiv b \equiv 0 \pmod{g}$, d'où le résultat. □

4.3 Construction de nos nouveaux protocoles de Distribution Quantique de Clés et de Partage de Secret pour qutrits

Pour $d = 3$, posons $\omega = \mathrm{e}^{\frac{2i\pi}{3}}$ et $\zeta = \mathrm{e}^{\frac{2i\pi}{9}}$ les racines troisièmes et neuvièmes de l'unité respectivement, vérifiant $\omega = \zeta^3$. Dans ce cas, pour $\zeta = \mathrm{e}^{\frac{2i\pi}{3g}}$, on choisit arbitrairement $g = 3$ pour maximiser le taux de génération de trits secrets.

Dans cette section, on utilisera une famille particulière de ditters dont les déphasages vérifient $\omega_k = \omega^k$ pour $k = 0, .., d-1$. Chaque participant est numéroté par $i = 1, ..., n$ et mesure des observables de la forme $Z_{\Theta_{(i),p}}$ qui correspondent à un tritter paramétré par les triplets de déphasages :

$$\Theta_{(i),p} = (1, \zeta^p, \zeta^{2p}) \qquad \text{pour} \qquad p = 0, 1, 2.$$

Avec ces tritters spécifiques et nos notions de mesures accordées et quasi-accordées, nous construisons deux nouveaux protocoles en dimension 3 entre n participants, pour $n = 2$ puis $n = 3$.

4.3.1 Protocole de Distribution Quantique de Clés pour $d = 3$ et $n = 2$

Nous utilisons l'état maximalement intriqué $|\psi_{\mathrm{GHZ}_2}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$ pour $d = 3$ et $n = 2$ décrit en (1.9).

Les deux participants Alice et Bob, numérotés respectivement par $i = 1, 2$, effectuent les mesures $A_{a_1 b_1}$ et $B_{a_2 b_2}$ correspondant aux observables produit $Z_{\Theta_{(1),a_1}} Z_{\Theta_{(1),b_1}}$ pour $(a_1, b_1) \in \{(0,0), (1,1), (0,1), (1,0)\}$ et $Z_{\Theta_{(2),a_2}} Z_{\Theta_{(2),b_2}}$ pour $(a_2, b_2) \in \{(0,0), (2,2), (0,2), (2,0)\}$ respectivement.

Concrètement, Alice et Bob choisissent entre quatre mesures correspondant aux ditters paramétrés par les déphasages suivants :

$$\begin{aligned} A_{00} &: (1,1,1) & B_{00} &: (1,1,1) \\ A_{11} &: (1,\zeta,\zeta^2) & B_{22} &: (1,\zeta^{-1},\zeta^{-2}) \\ A_{01} &: (\zeta^{-1},\zeta^{-2},1) & B_{02} &: (\zeta,\zeta^2,1) \\ A_{10} &: (\zeta^{-2},1,\zeta^{-1}) & B_{20} &: (\zeta^2,1,\zeta) \end{aligned}$$

Les déphasages correspondant aux mesures $A_{00}, A_{11}, B_{00}, B_{22}$ sont décrites dans [29] et sont également utilisées dans notre travail précédent [44].

Procédure :

1. Alice prépare des paires de qutrits intriqués dans l'état $|\psi_{\mathrm{GHZ}_2}\rangle$. Elle distribue un qutrit de chaque paire à Bob.
2. Alice et Bob effectuent sur chacun de leurs qutrits une mesure aléatoirement choisie parmi leurs quatre mesures $A_{a_1b_1}$ et $B_{a_2b_2}$ respectivement. Ils répètent ensuite les étapes 1 et 2 jusqu'à ce que toutes les mesures soient effectuées.
3. Alice et Bob annoncent publiquement leurs séquences de mesures, mais gardent toutes leurs issues secrètes.
4. D'après le théorème 5, pour chaque 2-uplets de mesures (a_1b_1, a_2b_2), Alice et Bob obtiennent un trit de clé secrète si ce 2-uplet vérifie la condition suivante :

$$a_1 + a_2 \equiv 0 \pmod 3 \qquad \text{et} \qquad b_1 + b_2 \equiv 0 \pmod 3. \tag{4.6}$$

5. Pour les 2-uplets ne vérifiant pas cette condition, Alice et Bob utilisent quand même une partie des issues correspondant à des choix de mesures spécifiques pour tester la sécurité en effectuant deux vérifications de la violation d'une même inégalité de Bell homogène. Les choix de mesure utilisés pour ces tests de sécurité et l'inégalité de Bell homogène à vérifier sont listés plus bas.
6. Si l'inégalité de Bell homogène n'exhibe pas de violation, la clé secrète est potentiellement compromise et doit être écartée. Alice et Bob recommencent alors la procédure.

Choix de mesure et violation de l'inégalité de Bell homogène :

Nous utilisons deux groupes de mesures C_1 et C_2 pour effectuer deux tests de sécurité en vérifiant la violation de l'inégalité de Bell suivante :

$$-\frac{2}{9}\mathrm{Re}(E(T_{\mathrm{QKD}d_3n_2})) \leqslant 1 \tag{4.7}$$

avec
$$\begin{aligned} T_{\mathrm{QKD}d_3n_2} = 3\big[&-\omega^2 a_1^2 a_2^2 + \omega a_1^2 a_2 b_2 + \omega a_1 b_1 a_2^2 + (1-\omega^2) a_1 b_1 a_2 b_2 \\ &- a_1 b_1 b_2^2 - b_1^2 a_2 b_2 + \omega^2 b_1^2 b_2^2\big]. \end{aligned}$$

Dans cette inégalité, les triplets de mesures (a_1^2, b_1^2, a_1b_1) sont à remplacer par les mesures d'Alice et les triplets de mesures (a_2^2, b_2^2, a_2b_2) par les mesures de Bob.

Les mesures d'Alice et Bob utilisées pour effectuer ces deux tests de sécurité sont décrites à la suite :

	Alice : (a_1, b_1, a_1b_1)	Bob : (a_2^2, b_2^2, a_2b_2)
C_1	$(A_{00},\ A_{11},\ A_{01}^2)$	$(B_{22},\ B_{00},\ B_{20}^2)$
C_2	$(A_{11},\ A_{00},\ A_{10}^2)$	$(B_{00},\ B_{22},\ B_{02}^2)$

Tableau 4.6 – Tests de sécurité pour le protocole QKDd_3n_2

Concrètement, on vérifie les deux inégalités suivantes, où les mesures d'Alice et Bob ont été remplacées suivant les configurations C_1 et C_2.

Configuration C_1 :

$$-\frac{2}{9}\mathrm{Re}(E(T_{\mathrm{QKD}d_3n_2})) \leqslant 1$$

avec $$T_{\mathrm{QKD}d_3n_2} = 3\big[-\omega^2 A_{00}^2 B_{22}^2 + \omega A_{00}^2 B_{20}^2 + \omega A_{01}^2 B_{22}^2 + (1-\omega^2) A_{01}^2 B_{20}^2 - A_{01}^2 B_{00}^2 - A_{11}^2 B_{20}^2 + \omega^2 A_{11}^2 B_{00}^2\big].$$

Configuration C_2 :

$$-\frac{2}{9}\mathrm{Re}(E(T_{\mathrm{QKD}d_3n_2})) \leqslant 1$$

avec $$T_{\mathrm{QKD}d_3n_2} = 3\big[-\omega^2 A_{11}^2 B_{00}^2 + \omega A_{11}^2 B_{02}^2 + \omega A_{10}^2 B_{00}^2 + (1-\omega^2) A_{10}^2 B_{02}^2 - A_{10}^2 B_{22}^2 - A_{00}^2 B_{02}^2 + \omega^2 A_{00}^2 B_{22}^2\big].$$

On a choisi ces mesures spécifiques car elles nous permettent de maximiser le taux de génération de clés d'après la condition obtenue dans le théorème 5. De plus, nous avons décidé d'effectuer des vérifications de cette inégalité parmi les $3^{3^2} = 19683$ inégalités de Bell homogènes existantes pour $d = 3$ et $n = 2$ car c'est celle qui nous permet d'obtenir, avec les paramètres choisis, la valeur de violation la plus haute.

Avec l'état maximalement intriqué $|\psi_{\mathrm{GHZ}_2}\rangle$, ces deux groupes de mesures C_1 et C_2 atteignent la même valeur de violation optimale $v \simeq 1.137$.

Résumé du protocole hQSSd3n2 :

Lorsque Alice et Bob effectuent leurs mesures respectives $A_{a_1b_1}$ et $B_{a_2b_2}$, les issues obtenues sont utilisées à différentes fins suivant la valeur du 2-uplet (a_1b_1, a_2b_2), qui peut prendre $4^2 = 16$ valeurs possibles.

- Lorsque $(a_1b_1, a_2b_2) \in \{(00,00),(11,22),(01,02),(10,20)\}$, ce qui représente **25**% des cas, ils récupèrent un trit de clé d'après la condition (4.6),

- Les 12 choix restants (75% des cas) sont utilisés pour effectuer deux tests de la violation d'une même inégalité de Bell homogène.

Ces différentes situations sont résumées dans le tableau suivant :

	B_{00}	B_{22}	B_{02}	B_{20}
A_{00}	k	(c_1, c_2)	c_2	c_1
A_{11}	(c_1, c_2)	k	c_2	c_1
A_{01}	c_1	c_1	k	c_1
A_{10}	c_2	c_2	c_2	k

k : Alice et Bob obtiennent un trit de secret.

c_1 et c_2 : Alice et Bob obtiennent des valeurs pour vérifier la violation de $T_{\text{QKD}d_3n_2}$.

Tableau 4.7 – Résumé du protocole QKDd_3n_2

4.3.2 Protocole de Partage de Secret Quantique pour $d = 3$ et $n = 3$

On utilise l'état maximalement intriqué $|\psi_{\text{GHZ}_3}\rangle$ pour $d = 3$ et $n = 3$ décrit en (1.9).

Les participants Alice, Bob et Charlie respectivement numérotés par $i = 1, 2, 3$ utilisent les mesures $A_{a_1b_1}$, $B_{a_2b_2}$ et $C_{a_3b_3}$. Les mesures d'Alice correspondent aux observables produit $Z_{\Theta_{(1),a_1}} Z_{\Theta_{(1),b_1}}$ pour $(a_1, b_1) \in \{(0,0), (1,1), (2,2), (0,1), (0,2), (1,2)\}$ et sont explicitées ci-dessous :

$$\begin{aligned} A_{00} &: (1,1,1) & A_{01} &: (\zeta^{-1}, \zeta^{-2}, 1) \\ A_{11} &: (1,\zeta,\zeta^2) & A_{02} &: (\zeta^{-2}, \zeta^{-4}, 1) \\ A_{22} &: (1,\zeta^2,\zeta^4) & A_{12} &: (\zeta^{-4}, \zeta^{-4}, \zeta^{-1}) \end{aligned}$$

Les mesures de Bob et Charlie sont identiques aux notations près en remplaçant (a_1, b_1) par (a_2, b_2) et (a_3, b_3) respectivement.

Procédure :

1. Alice prépare des qutrits intriqués dans l'état $|\psi_{\text{GHZ}_3}\rangle$. Elle garde un qutrit, en distribue un à Bob et le dernier à Charlie.
2. Alice, Bob et Charlie effectuent sur chacun de leurs qutrits une mesure aléatoirement choisie parmi leurs mesures $A_{a_1b_1}$, $B_{a_2b_2}$ et $C_{a_3b_3}$ respectivement. Ils répètent ensuite les étapes 1 et 2 jusqu'à ce que toutes les mesures soient effectuées.
3. Bob et Charlie annoncent publiquement leurs séquences de mesures, mais gardent toutes leurs issues secrètes.

4. D'après le théorème 5, pour chaque triplets de mesures (a_1b_1, a_2b_2, a_3b_3), Alice, Bob et Charlie obtiennent un trit de clé secrète si ce triplet vérifie la condition suivante :

$$a_1 + a_2 + a_3 \equiv 0 \pmod 3 \qquad \text{et} \qquad b_1 + b_2 + b_3 \equiv 0 \pmod 3. \tag{4.8}$$

   Alice détermine les triplets qui vérifient cette condition puis indique à Bob et Charlie quelles issues garder pour établir le secret commun.

Pour les triplets ne vérifiant pas cette condition, Alice, Bob et Charlie utilisent quand même une partie des issues correspondant à des choix de mesures spécifiques pour tester la sécurité en effectuant douze vérifications de la violation de cinq inégalités de Bell homogènes. Les choix de mesure utilisés pour ces tests de sécurité et les inégalités de Bell homogènes à vérifier sont listés plus bas.

Si l'une des inégalités de Bell homogènes n'exhibe pas de violation, la clé secrète est potentiellement compromise et doit être écartée. Alice, Bob et Charlie recommencent alors la procédure.

Choix de mesure et violation des inégalités de Bell homogènes :

On utilise douze groupes de mesures C_1 to C_{12} pour des tests de sécurité vérifiant la violation des inégalités de Bell homogènes suivantes, numérotées par $j = 1, .., 5$:

$$-\frac{2}{27}\mathrm{Re}(E(T_{j_{\mathrm{QSSd_3n_3}}})) \leqslant 1 \tag{4.9}$$

avec les polynômes homogènes $T_{j_{\mathrm{QSSd_3n_3}}}$ décrits ci-dessous.

$$\begin{aligned}
T_{1_{\mathrm{QSSd_3n_3}}} =& -6a_1^2a_2^2a_3^2 + (3\omega-6)a_1^2a_2^2a_3b_3 + 3a_1^2a_2b_2a_3^2 + 6a_1^2a_2b_2a_3b_3 \\
&+ (12\omega+6)a_1^2a_2b_2b_3^2 + (6\omega+6)a_1^2b_2^2a_3^2 + (3\omega-6)a_1^2b_2^2a_3b_3 \\
&+ (3\omega-3)a_1^2b_2^2b_3^2 + (3\omega+3)a_1b_1a_2^2a_3^2 + (-3\omega+3)a_1b_1a_2^2a_3b_3 \\
&+ 3\omega a_1b_1a_2^2b_3^2 - 3\omega a_1b_1a_2b_2a_3^2 + (-3\omega-6)a_1b_1a_2b_2a_3b_3 \\
&+ 3a_1b_1a_2b_2b_3^2 - 3\omega a_1b_1b_2^2a_3^2 + (3\omega-3)a_1b_1b_2^2a_3b_3 \\
&+ 3\omega a_1b_1b_2^2b_3^2 + 9\omega b_1^2a_2^2a_3^2 - 6\omega b_1^2a_2^2a_3b_3 - 3b_1^2a_2^2b_3^2 \\
&+ (6\omega+3)b_1^2a_2b_2a_3^2 + (-3\omega-3)b_1^2a_2b_2a_3b_3 \\
&+ 6b_1^2a_2b_2b_3^2 + (-3\omega-3)b_1^2b_2^2a_3b_3 - 3\omega b_1^2b_2^2b_3^2.
\end{aligned}$$

$$\begin{aligned}T_{2_{\mathrm{QSS}d_3n_3}} =&(-3\omega-6)a_1^2a_2^2a_3^2-3a_1^2a_2^2a_3b_3+3\omega a_1^2a_2^2b_3^2+(3\omega+6)a_1^2a_2b_2a_3^2\\&-3a_1^2a_2b_2a_3b_3+(-3\omega-3)a_1^2a_2b_2b_3^2-3a_1^2b_2^2a_3b_3+(9\omega+3)a_1^2b_2^2b_3^2\\&+3a_1b_1a_2^2a_3^2-9\omega a_1b_1a_2^2a_3b_3-3a_1b_1a_2^2b_3^2+(-3\omega-3)a_1b_1a_2b_2a_3^2\\&-9\omega a_1b_1a_2b_2a_3b_3+(-6\omega-6)a_1b_1a_2b_2b_3^2+3\omega a_1b_1b_2^2a_3^2+9\omega a_1b_1b_2^2a_3b_3\\&-3\omega a_1b_1b_2^2b_3^2-3\omega b_1^2a_2^2a_3^2-6\omega b_1^2a_2^2a_3b_3+(3\omega+3)b_1^2a_2b_2a_3^2\\&+(-6\omega-9)b_1^2a_2b_2a_3b_3+(3\omega+6)b_1^2a_2b_2b_3^2-3b_1^2b_2^2a_3^2\\&+(-6\omega-9)b_1^2b_2^2a_3b_3+(-3\omega+3)b_1^2b_2^2b_3^2.\end{aligned}$$

$$\begin{aligned}T_{3_{\mathrm{QSS}d_3n_3}} =\ &6\omega a_1^2a_2^2a_3^2-3\omega a_1^2a_2^2a_3b_3-3\omega a_1^2a_2^2b_3^2-6a_1^2a_2b_2a_3^2\\&+(3\omega+9)a_1^2a_2b_2a_3b_3+(-3\omega-3)a_1^2a_2b_2b_3^2+(6\omega+3)a_1^2b_2^2a_3^2\\&+(-6\omega-3)a_1^2b_2^2a_3b_3-6\omega a_1b_1a_2^2a_3^2+3a_1b_1a_2^2a_3b_3\\&+(-3\omega-3)a_1b_1a_2^2b_3^2+(-12\omega-6)a_1b_1a_2b_2a_3^2\\&+(-3\omega-6)a_1b_1a_2b_2a_3b_3+(-3\omega-6)a_1b_1a_2b_2b_3^2\\&+(3\omega-6)a_1b_1b_2^2a_3^2-3\omega a_1b_1b_2^2a_3b_3-3a_1b_1b_2^2b_3^2\\&+(3\omega+6)b_1^2a_2^2a_3b_3+(6\omega-6)b_1^2a_2^2b_3^2+(-6\omega-6)b_1^2a_2b_2a_3^2\\&-3b_1^2a_2b_2a_3b_3-3\omega b_1^2a_2b_2b_3^2+3b_1^2b_2^2a_3^2+3b_1^2b_2^2a_3b_3+3b_1^2b_2^2b_3^2.\end{aligned}$$

$$\begin{aligned}T_{4_{\mathrm{QSS}d_3n_3}} =&-3\omega a_1^2a_2^2a_3^2+9a_1^2a_2^2a_3b_3+(3\omega+9)a_1^2a_2^2b_3^2+(6\omega+3)a_1^2a_2b_2a_3^2\\&-6\omega a_1^2a_2b_2a_3b_3+6a_1^2a_2b_2b_3^2+3a_1^2b_2^2a_3^2-3a_1^2b_2^2a_3b_3+(3\omega+6)a_1b_1a_2^2a_3^2\\&+(-15\omega-9)a_1b_1a_2^2a_3b_3+(3\omega+3)a_1b_1a_2^2b_3^2+3\omega a_1b_1a_2b_2a_3^2\\&-3\omega a_1b_1a_2b_2a_3b_3+9\omega a_1b_1a_2b_2b_3^2-3\omega a_1b_1b_2^2a_3^2+(3\omega-3)a_1b_1b_2^2a_3b_3\\&+3a_1b_1b_2^2b_3^2+(6\omega+6)b_1^2a_2^2a_3^2+(3\omega+3)b_1^2a_2^2a_3b_3-3\omega b_1^2a_2b_2a_3^2\\&+(-3\omega-6)b_1^2a_2b_2a_3b_3+(-3\omega-3)b_1^2a_2b_2b_3^2+3\omega b_1^2b_2^2a_3b_3-3\omega b_1^2b_2^2b_3^2.\end{aligned}$$

$$\begin{aligned}T_{5_{\mathrm{QSS}d_3n_3}} =&-6\omega a_1^2a_2^2a_3^2-3\omega a_1^2a_2^2a_3b_3+(3\omega+3)a_1^2a_2b_2a_3^2+(-3\omega+3)a_1^2a_2b_2a_3b_3\\&-6a_1^2a_2b_2b_3^2+3\omega a_1^2b_2^2a_3b_3+6\omega a_1^2b_2^2b_3^2+(9\omega+6)a_1b_1a_2^2a_3^2\\&+(6\omega+3)a_1b_1a_2^2a_3b_3+3\omega a_1b_1a_2^2b_3^2+(6\omega+3)a_1b_1a_2b_2a_3^2+3\omega a_1b_1a_2b_2a_3b_3\\&-3a_1b_1a_2b_2b_3^2-6a_1b_1b_2^2a_3^2+6\omega a_1b_1b_2^2a_3b_3+(-6\omega-3)a_1b_1b_2^2b_3^2+12b_1^2a_2^2a_3b_3\\&-3b_1^2a_2^2b_3^2+3\omega b_1^2a_2b_2a_3^2+(3\omega-6)b_1^2a_2b_2a_3b_3+(-6\omega-3)b_1^2a_2b_2b_3^2\\&+(3\omega+3)b_1^2b_2^2a_3^2+(3\omega-3)b_1^2b_2^2a_3b_3-6\omega b_1^2b_2^2b_3^2.\end{aligned}$$

Dans ces inégalités, les triplets de mesures (a_1^2, b_1^2, a_1b_1), (a_2^2, b_2^2, a_2b_2) et (a_3^2, b_3^2, a_3b_3) doivent être remplacés par les mesures d'Alice, Bob et Charlie respectivement.

Les choix de mesure utilisés pour effectuer ces douze tests de sécurité ainsi que les polynômes homogènes $T_{j_{\mathrm{QSS}d_3n_3}}$ et les valeurs de violation v correspondant à chaque choix sont décrits ci-dessous :

	Alice : (a_1^2, b_1^2, a_1b_1)	Bob : (a_2^2, b_2^2, a_2b_2)	Charlie : (a_3^2, b_3^2, a_3b_3)	j	v
C_1	$(A_{00},\ A_{11},\ A_{01})$	$(B_{11},\ B_{22},\ B_{12})$	$(C_{00},\ C_{22},\ C_{02})$	1	$1,648$
C_2	$(A_{11},\ A_{22},\ A_{12})$	$(B_{00},\ B_{22},\ B_{02})$	$(C_{00},\ C_{11},\ C_{01})$	2	$1,369$
C_3	$(A_{00},\ A_{22},\ A_{02})$	$(B_{00},\ B_{11},\ B_{01})$	$(C_{11},\ C_{22},\ C_{12})$	3	$1,253$
C_4	$(A_{00},\ A_{11},\ A_{01})$	$(B_{00},\ B_{22},\ B_{02})$	$(C_{11},\ C_{22},\ C_{12})$	2	$1,369$
C_5	$(A_{11},\ A_{22},\ A_{12})$	$(B_{00},\ B_{11},\ B_{01})$	$(C_{00},\ C_{22},\ C_{02})$	1	$1,648$
C_6	$(A_{00},\ A_{22},\ A_{02})$	$(B_{11},\ B_{22},\ B_{12})$	$(C_{00},\ C_{11},\ C_{01})$	3	$1,253$
C_7	$(A_{00},\ A_{11},\ A_{01})$	$(B_{00},\ B_{11},\ B_{01})$	$(C_{11},\ C_{22},\ C_{12})$	4	$1,269$
C_8	$(A_{00},\ A_{11},\ A_{01})$	$(B_{11},\ B_{22},\ B_{12})$	$(C_{00},\ C_{11},\ C_{01})$	4	$1,269$
C_9	$(A_{00},\ A_{11},\ A_{01})$	$(B_{11},\ B_{22},\ B_{12})$	$(C_{11},\ C_{22},\ C_{12})$	5	$1,516$
C_{10}	$(A_{11},\ A_{22},\ A_{12})$	$(B_{00},\ B_{11},\ B_{01})$	$(C_{00},\ C_{11},\ C_{01})$	4	$1,269$
C_{11}	$(A_{11},\ A_{22},\ A_{12})$	$(B_{00},\ B_{11},\ B_{01})$	$(C_{11},\ C_{22},\ C_{12})$	5	$1,516$
C_{12}	$(A_{11},\ A_{22},\ A_{12})$	$(B_{11},\ B_{22},\ B_{12})$	$(C_{00},\ C_{11},\ C_{01})$	5	$1,516$

Tableau 4.8 – Tests de sécurité pour le protocole QSSd_3n_3

Nous avons choisi ces mesures spécifiques car elles maximisent le taux de génération de trits secrets d'après le condition obtenue dans le théorème 5. De plus, étant donné qu'il nous a été impossible de tester l'ensemble des 3^{3^3} inégalités de Bell homogènes existantes par manque de puissance de calcul, nous avons décidé de vérifier ces cinq inégalités car elles nous permettaient d'obtenir les valeurs de violation les plus hautes pour chaque choix de mesure parmi les inégalités testées.

Résumé du protocole hQSSd3n3 :

Lorsque Alice, Bob et Charlie effectuent leurs mesures respectives $A_{a_1b_1}$, $B_{a_2b_2}$ et $C_{a_3b_3}$, les issues obtenues sont utilisées à des fins différentes selon les valeurs du triplet (a_1b_1, a_2b_2, a_3b_3) qui peut prendre $6^3 = 216$ valeurs possibles.

- Pour 24 choix de (a_1b_1, a_2b_2, a_3b_3), ce qui représente $\mathbf{11,11}\%$ des cas, ils produisent un trit secret d'après la condition (4.8),
- 153 choix sont impliqués dans la vérification d'au moins une des cinq inégalités de Bell homogènes ($\mathbf{70,83}\%$ des cas),
- 39 choix sont inutilisés ($\mathbf{18,05}\%$ des cas).

Analyse du coût :

Supposons qu'Alice, Bob et Charlie souhaitent partager une séquence de trits de longueur m. Nous allons maintenant évaluer le nombre de particules et de nombres aléatoires générés et transmis lors de notre protocole.

- Qutrits intriqués préparés et transmis par Alice : $3m$ et $2m$,
- Nombre aléatoires générés et mesures effectuées : $3m$,
- Séquences de mesures révélées à Alice : $2m$,
- Taille des séquences transmises par Alice pour indiquer les mesures valides, les mesures servant à tester les inégalités et les mesures inutilisées : $2m$.

Conclusion :

Dans la première partie de ce chapitre, nous avons décrit le protocole NDEB pour qudits, extension du protocole E91 pour qubits à des systèmes de dimension d. En particulier, la sécurité de ce protocole contre les attaques par clonage se base sur la violation de l'inégalité CGLMP-d. Nous avons ensuite présenté notre nouvelle famille de protocoles hdDEB pour qudits dont la sécurité contre les attaques par clonage se base sur des inégalités de Bell homogène, ce qui nous a permis d'obtenir une meilleure résistance au bruit pour le même niveau de sécurité que le protocole NDEB.

Dans la seconde partie de ce chapitre, notre objectif était de décrire un environnement général servant à construire des protocoles de Partage de Secret Quantique à l'aide de mesures faites par des ditters, en nous inspirant du protocole pour Bases Sans Biais décrit par Yu *et al.* dans [53].

En définissant deux nouvelles notions, les mesures accordées et quasi-accordées, qui établissent un lien entre les déphasages d'un groupe de ditters, nous avons exhibé un critère sur les mesures à choisir pour maximiser le taux de génération de dits secrets dans les protocoles de Partage de Secret. Nous avons également explicité ce critère pour le cas $d = 3$ et $n = 2, 3$ afin de construire des nouveaux protocoles de Distribution Quantique de Clés et de Partage de Secret Quantique, nommés respectivement hQSSd3n2 et hQSSd3n3.

Bibliographie

[1] F. Arnault, "A complete set of multidimensional Bell inequalities." *Journal of Physics A*, vol. 45, p. 255304, 2012.

[2] M. Żukowski, A. Zeilinger, and M. Horne, "Realizable higher-dimensional two-particle entanglements via multiport beam splitters." *Physical Review A*, vol. 55, p. 2564, 1997.

[3] F. Arnault and Z. Amblard, "A quantum key distribution protocol for qudits with better noise resistance." 2015, arXiv e-print : 1504.08161.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Information and Quantum Computation.* Cambridge University Press, 2010.

[5] M. Ghil and J. Roux, *Mathématiques Appliquées Aux Sciences De La Vie Et De La Planète : Cours Et Exercices Corrigés.* Dunod, 2010.

[6] E. T. Browne, "The characteristic equation of a matrix." *Bulletin of the American Mathematical Society*, vol. 34, p. 363, 1928.

[7] A. Hjørungnes, *Complex-Valued Matrix Derivatives : With Applications in Signal Processing and Communications.* Cambridge University Press, 2011.

[8] K. Mattle, M. Michler, H. Weinfurter, A. Zeilinger, and M. Żukowski, "Non-classical statistics at multiport beam splitters." *Applied Physics B*, vol. 60, p. S111, 1995.

[9] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Multiparticle interferometry and the superposition principle." *Physics Today*, vol. 46, p. 22, 1993.

[10] J. Schwinger, "Unitary operator bases." *Proc. Natl. Acad. Sci. USA*, vol. 46, p. 570, 1960.

[11] J. L. Carter and M. N. Wegman, "Universal classes of hash functions." *Journal of Computer and System Sciences*, vol. 18, no. 2, p. 143, 1979.

[12] ——, "New hash functions and their use in authentication and set equality." *Journal of Computer and System Sciences*, vol. 22, no. 3, p. 265, 1981.

[13] D. R. Stinson, "Universal hashing and authentication codes." *Designs, Codes and Cryptography*, vol. 4, no. 3, p. 369, 1994.

[14] C. H. Bennett and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing." in *International Conference on Computers, Systems & Signal Processing, Bangalore, India*, 1984, p. 175.

[15] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states." *Phys. Rev. Lett.*, vol. 81, no. 14, p. 3018, 1998.

[16] A. K. Ekert, "Quantum cryptography based on Bell's theorem." *Physical Review Letters*, vol. 67, p. 661, 1991.

[17] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem." *Phys. Rev. Lett.*, vol. 68, no. 5, p. 557, 1992.

[18] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger, "Feasibility of 300 km quantum key distribution with entangled states." *New Journal of Physics*, vol. 11, p. 085002, 2009.

[19] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.

[20] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photonics*, vol. 3, pp. 696–705, 2009.

[21] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," *Optics Express*, vol. 21, no. 25, pp. 31 395–31 401, 2013.

[22] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution." *Journal of Modern Physics*, vol. 81, p. 1301, 2009.

[23] A. Bocquet, *Modèles de sécurité réalistes pour la distribution quantique de clés*, <pastel 00784705>, Ed. Télécom ParisTech, 2011.

[24] L. Bacsardi, A. Kiss, M. Galambos, and S. Imre, "Examining quantum key distribution protocols in laser based satellite communications," *Communication, Networks and Satellite (ComNetSat)*, 2012.

[25] C. W. Lim, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Random variation of detector efficiency : A countermeasure against detector blinding attacks for quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 192–196, 2015.

[26] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 93, p. 230504, 2005.

[27] J.-L. Chen, D. Kaszlikowski, L. C. Kwek, and C. H. Oh, "Wringing out new Bell inequalities for three-dimensional systems (qutrits)." *Modern Physics Letters A*, vol. 17, p. 2231, 1989.

[28] T. Durt, D. Kaszlikowski, J. Chen, and L. Kwek, "Security of quantum key distribution with entangled qudits." *Physical Review A*, vol. 69, p. 032313, 2004.

[29] A. Acín, T. Durt, N. Gisin, and J. I. Latorre, "Quantum non-locality in two three level systems." *Physical Review A*, vol. 65, p. 052325, 2002.

[30] J. L. Chen, D. Kaszlikowski, L. C. Kwek, C. H. Oh, and M. Żukowski, "Entangled three-state systems violate local realism more strongly than qubits : an analytical proof." *Physical Review A*, vol. 64, p. 052109, 2001.

[31] J. Durt, D. Kaszlikowski, and M. Żukowski, "Violations of local realism with quantum systems described by N-dimensional Hilbert spaces up to N = 16." *Physical Review A*, vol. 64, p. 024101, 2001.

[32] I. Jex, S. Stenholm, and A. Zeilinger, "Hamiltonian theory of a symmetric multiport." *Opt. Comm.*, vol. 117, p. 95, 1995.

[33] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, "Bell inequalities for arbitrarily high-dimensional systems." *Phys. Rev. Lett.*, vol. 88, p. 040404, 2002.

[34] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned." *Nature*, vol. 299, no. 5886, p. 802, 1982.

[35] P. W. Shor and J. Preskill., "Simple proof of security of the BB84 quantum key distribution protocol." *Phys. Rev. Lett.*, vol. 85, p. 441, 2000.

[36] V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee, "A comparative study of protocols for secure quantum communication under noisy environment : single-qubit-based protocols versus entangled-state-based protocols." March 2016, arXiv :1603.00178.

[37] H. Inamori, L. Rallan, and V. Vedral, "Security of EPR-based quantum cryptography against incoherent symmetric attacks." *Journal of Physics A*, vol. 34, no. 35, p. 6913, 2001.

[38] X. Ma, C. H. F. Fung, and H. K. Lo, "Quantum key distribution with entangled photon sources." *Phys. Rev. A*, vol. 76, p. 012307, 2007.

[39] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, "Security of entanglement-based quantum key distribution with practical detectors." April 2008, arXiv e-print : 0804.0891.

[40] R. Y. Q. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution." *New Journal of Physics*, vol. 11, p. 045024, 2009.

[41] S.-W. Ji, J. Lee, J. Lim, K. Nagata, and H.-W. Lee, "Multisetting Bell inequality for qudits." *Physical Review A*, vol. 78, no. 5, p. 052103, Nov 2008.

[42] Y.-C. Liang, C.-W. Lim, and D.-L. Deng, "Reexamination of a multisetting Bell inequality for qudits." *Physical Review A*, vol. 80, no. 5, p. 052116, Nov 2009.

[43] T. Durt, N. J. Cerf, N. Gisin, and M. Żukowski, "Security of quantum key distribution with entangled qutrits." *Physical Review A*, vol. 67, p. 012311, 2003.

[44] F. Arnault and Z. Amblard, "A qutrit quantum key distribution protocol using Bell inequalities with larger violation capabilities." *Quantum Information and Computation*, vol. 15, No 15 & 16, pp. 1295–1306, 2015.

[45] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing." *Phys. Rev. A*, vol. 63, p. 042301, 2001.

[46] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C-Y.Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, "Experimental quantum secret sharing and third-man quantum cryptography." *Phys. Rev. Lett.*, vol. 95, p. 200502, 2005.

[47] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, "Tripartite quantum state sharing." *Phys. Rev. Lett.*, vol. 92, p. 177903, 2004.

[48] A. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. Ralph, and P. K. Lam, "Continuous variable quantum state sharing via quantum disentanglement." *Phys. Rev. A*, vol. 71, p. 033814, 2005.

[49] G.-P. Guo and G.-C. Guo, "Quantum secret sharing without entanglement." *Physics Letters A*, vol. 310, p. 247, 2003.

[50] Y. Sun, F. Gao, Z. Yuan, Y.-B. Li, and Q.-Y. Wen, "Splitting a quantum secret without the assistance of entanglements." *Quantum Information Processing*, vol. 11, p. 1741, 2012.

[51] M. Hillary, V. Bužek, and A. Berthiaume, "Quantum secret sharing." *Physical Review A*, vol. 59, p. 1829, 1999.

[52] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting." *Physical Review A*, vol. 59, p. 162, 1999.

[53] I.-C. Yu, F.-L. Lin, and C.-Y. Huang, "Quantum secret sharing with multi-level Mutually (Un-)biased Bases." *Physical Review A*, vol. 78, p. 012344, 2008.

[54] V. Scarani and N. Gisin, "Quantum communication between N partners and Bell's inequalities." *Phys. Rev. Lett.*, vol. 87, p. 117901, 2001.

[55] ——, "Quantum key distribution between N partners : Optimal eavesdropping and Bell's inequalities." *Phys. Rev. A*, vol. 65, no. 012311, 2001.

[56] A. Sen, U. Sen, and M. Żukowski, "Unified criterion for security of secret sharing in terms of violation of Bell inequalities." *Phys. Rev. A*, vol. 68, p. 032309, 2003.

Conclusion

Les inégalités de Bell occupent une place importante dans la sécurité des protocoles basés sur l'intrication quantique. Le premier objectif de cette thèse était d'étudier les propriétés théoriques d'une nouvelle famille d'inégalités appelées inégalités de Bell homogènes en dimension d pour n parties et décrites par François Arnault dans [1]. L'étude de ces inégalités devait permettre d'exploiter les valeurs de violation élevées qu'elles atteignent dans des protocoles de Distribution Quantique de Clés et de Partage de Secret Quantique.

Afin de pouvoir implémenter les inégalités de Bell homogènes, nous avons étudié certaines propriétés des dispositifs optiques appelés *ditters*, utilisés pour mesurer des observables quantiques en dimension d. Ces ditters sont paramétrés par des déphasages qui déterminent les bases de mesures utilisées dans un protocole.

Notre première contribution à ce sujet, nécessaire à l'utilisation des inégalités de Bell homogènes dans un contexte expérimental, a été de formuler mathématiquement le produit de deux observables mesurées par des ditters et de montrer que ce produit correspond à une nouvelle mesure effectuée par un troisième ditter dont nous avons précisé les déphasages.

Par la suite, nous avons cherché à choisir judicieusement les déphasages de ces ditters de façon à optimiser le taux de génération de clés de nos protocoles, ce qui nous a conduit à notre seconde contribution : les notions de mesures accordées et mesures quasi-accordées. Ces deux nouvelles notions nous ont permis d'obtenir des critères sur le choix des déphasages optimisant le taux de génération de clés.

Grâce à ces nouvelles propriétés des ditters, nous avons conçu quatre protocoles : les protocoles de Distribution Quantique de Clés hQSSd3n2 et h3DEB pour qutrits, le protocole de Partage de Secret Quantique hQSSd3n3 pour qutrits et le protocole de Distribution Quantique de Clés hdDEB pour qudits basé sur les protocoles NDEB pour qudits décrits par Durt *et al* dans [28]. En particulier, l'utilisation des inégalités de Bell homogènes dans les protocoles hdDEB pour $d = 3, 4, 5$ a permis, grâce aux valeurs de violation élevées qu'elles atteignent, d'augmenter significativement la quantité de bruit tolérée par les protocole NDEB tout en gardant le même niveau de sécurité contre les attaques dites par clonage optimal.

Indépendamment de ces travaux sur les ditters, nous avons déterminé une borne supérieure sur la valeur de violation maximale atteinte par les inégalités de Bell homogènes en dimension d pour n parties. Nous avons également fait le lien entre certaines de nos inégalités de Bell homogènes pour qutrits et l'inégalité de Bell pour qutrits à trois mesures par parties décrite par Ji *et al* dans [41]. Nous avons recalculé les bornes classiques de l'inégalité de Ji *et al* en exploitant des relations entre les bases de mesure utilisées, ce qui nous a permis d'augmenter sa valeur de violation pour les paramètres considérés dans [41].

Nos travaux sur les inégalités de Bell homogènes et sur les propriétés des ditters ont résulté en la conception de plusieurs nouveaux protocoles de Distribution Quantique de Clés et de Partage de Secret Quantique. En particulier, nos protocoles hdDEB disposent d'une meilleure résistance au bruit que la famille des protocoles NDEB pour le même critère de sécurité. Nous avons également décrit deux nouvelles notions de mesures accordées et quasi-accordées qui facilitent l'obtention de critères pour le choix des bases de mesure à utiliser dans les protocoles de Partage de Secret Quantique, en vue d'augmenter le taux de génération de clés.

Nos recherches concernant les inégalités de Bell homogènes ont été limitées par la puissance de calcul dont nous disposions car, pour un d et un n fixés, on compte d^{d^n} inégalités de Bell homogènes à considérer. De plus, la valeur de violation atteinte par chacune de ces inégalités peut varier suivant le choix de l'état intriqué et les bases de mesures utilisées. En raison de ce trop grand nombre de paramètres, nous nous sommes limités aux dimensions $d = 3, 4, 5$ et aux cas de deux ou trois participants. A l'heure actuelle, nous manquons de critères pour choisir les inégalités les plus intéressantes en fonction de l'application souhaitée.

Dans nos nouveaux protocoles, nous nous sommes limités à la sécurité contre les attaques dites par clonage optimal décrites par Durt *et al* dans [28]. Nous ignorons si cette attaque est l'attaque optimale pour les protocoles hdDEB et une analyse de sécurité plus poussée reste à faire. Il serait également intéressant d' évaluer le bruit supplémentaire lié à l'ajout de nouvelles bases de mesures par rapport aux quatre bases de mesure des protocoles NDEB, ce qui peut varier en fonction de l'implémentation.

Concernant nos recherches sur les ditters et les mesures accordées et quasi-accordées, nous avons dérivé un critère pour optimiser le taux de génération de clés en nous limitant à une famille de bases de mesure spécifiques paramétrées par des puissances successives de phases. A l'heure actuelle, nous n'avons pas encore de critère pour optimiser le taux de génération de clés à partir de bases quelconques.

Cryptographie quantique et applications spatiales.

Résumé : Cette thèse réalisée en collaboration avec l'entreprise Thales Alenia Space, qui étudie les protocoles de cryptographie quantique à n parties en dimension d, a un double objectif. D'une part, nous analysons la famille des inégalités de Bell homogènes introduites par François Arnault dans [1] afin de proposer des outils théoriques pour leur compréhension et leur implémentation à l'aide d'appareils optiques appelés ditters dont une représentation mathématique est donnée par Żukowski *et al.* dans [2]. Avec ces outils théoriques, nous proposons de nouveaux protocoles cryptographiques en dimension d qui sont décrits dans [3] et qui utilisent ces inégalités. D'autre part, nous étudions les avantages et inconvénients de la cryptographie quantique pour la protection des communications avec un satellite LEO en environnement bruité.

Mots clés : Distribution Quantique de Clés, intrication, satellites.

Quantum cryptography and applications to space communications.

Abstract : This thesis in collaboration with Thales Alenia Space studies quantum cryptographic protocols for n parties in dimension d. We first analyze the family of Bell inequalities called homogeneous Bell inequalities introduced by François Arnault in [1] and we construct several theoretical tools for a better understanding of these inequalities. With these tools, we show how to implement the measurements required to test these inequalities by using optical devices calleds multiport beamsplitters and described by Żukowski *et al.* in [2]. We use these devices to construct new cryptographic protocols in dimension d called hdDEB which we describe in [3]. Then, we study advantages and drawbacks of the use of quantum cryptography to protect satellite links in a noisy environment.

Keywords : Quantum key distribution, entanglement, satellites.

XLIM - UMR CNRS n° 7252
123, Avenue Albert Thomas - 87060 LIMOGES