République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université A. Mira de Bejaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de Master Recherche en Informatique

Option : Intelligence Artificielle

Thème

Partage de secret quantique

Réalisé par

M^{lle} BENLAMARA Kamilia

Soutenu le 10/10/2021 devant le jury composé de

Nom et Prénom	**Grade**	**Établissement**	
M. AKILAL Abdellah	MAA	Université de Bejaia	Président
M. GHARBI Abdelhakim	Professeur	Université de Bejaia	Examinateur
Mme ZEBBOUDJ Sofia	MAB	Université de Bejaia	Encadrante
Mme BOUCHELAGHEM Siham	MAB	Université de Bejaia	Co-encadrante

Année Universitaire : 2020 - 2021

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

Bit	Binary digit
CSS	Classical Secret Sharing
EPR	Einstein-Podolsky-Rosen
GHZ	Greenberger-Horne-Zeilinger
QSS	Quantum Secret Sharing
Qubit	Quantum bit
SS	Secret Sharing

Remerciements

Je souhaiterai tout d'abord, remercier ALLAH le tout puissant de m'avoir donnée la force, le courage et la volonté d'accomplir ce modeste travail.

Ce travail n'aurait pas pu voir le jour sans l'aide et l'encadrement de Mme ZEBBOUDJ Sofia et de Mme BOUCHELAGHEM Siham, je tiens à les remercier sincèrement pour la qualité de leur encadrement exceptionnel, pour leur gentillesse, leurs conseils, leur bienveillance et surtout leur patience et leur disponibilité durant toutes les procédures de préparation de ce mémoire.

Je tiens à adresser mes sincères et vifs remerciements aux membres de jury pour l'honneur qu'ils m'ont fait en acceptant de siéger à ma soutenance.

Mes profonds remerciements vont également à toutes les personnes qui m'ont soutenue, aidé et participé de près ou de loin à la réalisation de ce mémoire. J'espère que vous trouverez à travers ces lignes, les sentiments de ma profonde reconnaissance.

Enfin, je ne peux passer outre ma reconnaissance envers mes parents, mon frère, ma chère jumelle pour leur patience, leur aide et soutien constant qui m'ont boostée à faire de mon mieux.

Dédicaces

Je dédie ce modeste travail

À ma très chère mère et mon adorable père

À ma très chère jumelle Wissam

À mon très chère frère Amrane

À toute ma famille

À tous mes amis.

Introduction générale

Dans tous les domaines, le partage de l'information est une activité courante qui détient un rôle de la plus haute importance. Or, la distance se dresse comme un rempart à l'accomplissement de cette tâche dans le cas où l'information devrait être partagée entre des individus se trouvant éloignés les uns des autres. De ce fait, le partage à distance devient une exigence qui doit être satisfaite. C'est alors que l'informatique est arrivée pour répondre à cette exigence en fournissant un accès de partage à distance où les informations sont transmises sous forme orale (par vocal) ou sous forme visuelle (schémas, images, animations, etc.).

De par leur nature, certaines informations qui doivent être partagées sont considérées comme des secrets qui ne devraient être connus que des parties concernées, et c'est ainsi que la sécurisation du partage devient obligatoire pour maintenir la confidentialité de ces informations. Le besoin de garantir la sécurisation du partage de secret n'est pas un besoin qui s'est fait ressentir qu'à notre époque, bien au contraire ce besoin remonte à des époques bien lointaines de la nôtre. Tout a commencé dans l'antiquité avec l'apparition des cités dirigées par des rois nommés par les citoyens pour régner et assurer la prospérité de leur cité. Cependant, ces cités se faisaient souvent la guerre, en général pour agrandir leur territoire ou pour les défendre contre des ennemis qui voulaient s'en acquérir. En cas de guerre, le besoin d'échanger des informations dont seul l'envoyeur et le destinataire pourraient comprendre le sens est primordiale afin de ne pas risquer qu'elles tombent entre de mauvaises mains, à cette époque le domaine de la cryptographie est né pour répondre a ce besoin on propososants divers protocoles permetant le partage de secrets où le sens n'est compris que par les personnes concernées.

L'être humain est toujours dans un état d'évolution ce qui conduit au développement des moyens utilisés pour le partager du secret. De ce fait, la cryptographie a perfectionné ses protocoles parallèlement aux progrès de l'homme pour pouvoir assurer un partage de secret sécurisé. D'où la naissance du sous-domaine de la cryptographie qui est le domaine du partage de secret quantique et sur lequel repose la problématique traitée dans ce mémoire. En effet, l'objectif de ce mémoire est la proposition d'un nouveau protocole de partage de secret quantique.

Pour mieux présenter notre travail, nous avons jugé utile de diviser ce rapport en trois (03) chapitres structurés de la manière suivante :

- ✓ Le premier chapitre est un chapitre introductif qui a pour but l'acquisition de toutes les notions et définitions requises pour la compréhension de sujet traité dans ce mémoire.

- ✓ Dans le deuxième chapitre, nous analyserons quelques travaux de recherche dans le domaine du partage quantique de secret, ce qui nous permettra par la suite de rédiger notre état de l'art.

- ✓ Dans le troisième et dernier chapitre, nous ferons la présentation du protocole de partage de secret quantique que nous avons proposé ainsi que sa validation.

Enfin, nous clôturerons ce mémoire avec une conclusion générale résumant l'essentiel de notre travail ainsi que quelques perspectives.

Chapitre 1

Notions préliminaires d'informatique quantique

1.1 Introduction

Ce premier chapitre introductif vise à faciliter la compréhension de certains aspects de la thématique abordée dans ce rapport. De ce fait, ce chapitre contient tous les concepts et définitions sur lesquels repose notre projet. Pour commencer, nous parcourerons le domaine de l'informatique en parlant de ses deux variantes, à savoir l'informatique classique et l'informatique quantique. Nous évoquerons ensuite des notions spécifiques appartenant à l'informatique quantique et ferons une comparaison entre ces deux variantes. Nous parlerons ensuite de cryptographie et de ses principales techniques, puis nous aborderons un sous-domaine spécifique de la cryptographie qu'est le partage de secret.

1.2 Une nouvelle étape pour l'informatique

L'informatique est la science du traitement des informations avec des moyens électroniques. Elle est conçue pour servir les humains. Elle s'ouccupe d'enregistrer, de stocker, de traiter, d'organiser, de transférer et de présenter les informations sous une forme utilisable pour les humains ainsi que pour la machine[18].

1.2.1 Informatique classique

Un ordinateur classique est une machine capable d'exécuter des opérations pour réaliser des calculs sur la base de la logique binaire [10].

L'unité de mesure de base de l'information en informatique classique est le bit, contraction de *binary digit*. Il désigne l'unité la plus simple utilisée dans un système de numération. Cette unité, directement associée au système binaire, ne peut prendre que deux valeurs ; 0 et 1. En informatique, le bit définit de façon plus précise une quantité minimale d'information pouvant être transmise par un message. On emploie alors le bit comme unité de mesure de base de l'information [1].

1.2.2 Informatique quantique

L'informatique quantique est le sous-domaine de l'informatique qui traite des calculateurs quantiques utilisant des phénomènes de la mécanique quantique, par opposition à ceux de l'électricité exclusivement, pour l'informatique dite classique. Les phénomènes quantiques utilisés sont l'intrication quantique et la superposition. Les opérations ne sont plus basées sur la manipulation des bits dans un état 0 ou 1, mais de qubits en superposition d'états 0 et/ou 1 [3].

Un ordinateur quantique est l'équivalent des ordinateurs classiques mais qui effectuerait ses calculs en utilisant directement les lois de la physique quantique et, à la base, celle dite de superposition des états quantiques [22].

L'unité de mesure de base de l'information en informatique quantique est le qubit (q-bit ou bit quantique), qui exploite les caractéristiques physiques de la matière subatomique. Son atout majeur est de pouvoir stocker plusieurs informations simultanément, là où les bits classiques n'en stockent qu'une seule [7].

1.2.3 Comparaison

Si l'informatique classique s'appuie sur les bits, l'informatique quantique repose sur les bits quantiques, ou qubits. À la différence du bit, le qubit n'est pas cantonné aux seuls 0 et 1, puisqu'il est capable de prendre ces deux valeurs à un même instant. C'est ce qu'on appelle le principe de superposition des états. Mais ce n'est pas la seule particularité de ces éléments car deux qubits peuvent également interagir, leurs états s'entremêlant et devenant interdépendants, on parle alors d'intrication [14].

Une autre caractéristique propre aux qubits est le non-clonage. Pour un bit classique, il est facile de réaliser une copie qui aura la même valeur que le bit original. Cependant cette opération, qui paraît en soi simple, est extrêmement difficile à réaliser avec un qubit. En effet, pour pouvoir faire une copie d'un qubit, il faudrait d'abord le mesurer. Comme mentionné précédemment avec le principe de superposition, un qubit peut prendre les valeurs 0 et 1 en même temps. Or, la mesure de ce dernier lui imposera l'une des valeurs 0 ou 1, au lieu des deux à la fois, ce qui entraînera inévitablement la modification de l'état original.

Dans certains cas, un ordinateur quantique peut faire des calculs beaucoup plus rapidement qu'un ordinateur classique. Avec un ordinateur classique, le temps croît exponentiellement avec la complexité du problème. Heureusement, cette croissance n'est que polynomiale pour un système quantique. [9]

1.3 Notions d'informatique quantique

Dans cette section, nous présentons certaines notions de base liées à l'informatique quantique qui nous seront utiles pour mieux appréhender notre problématique.

1.3.1 État d'un qubit

L'état d'un qubit unique peut être décrit par un vecteur colonne à deux dimensions de norme unitaire, c'est-à-dire ; que la somme des carrés des amplitudes de ses entrées doit être égale à 1. Ce vecteur, appelé vecteur d'état quantique, contient toutes les informations nécessaires pour décrire le système quantique à un qubit [5].

Tout vecteur colonne à deux dimensions de nombres réels ou complexes de norme 1 représente un état quantique possible contenu par un qubit. Ainsi,

$\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$ représente l'état d'un qubit, si α et β sont des nombres complexes satisfaisant

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

Voici quelques exemples de vecteurs d'état quantique valides représentant des qubits :

$$\begin{bmatrix}0\\ 1\end{bmatrix}, \begin{bmatrix}1\\ 0\end{bmatrix}, \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} \text{ et } \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}.$$

Les vecteurs d'état quantique $\begin{bmatrix}0\\ 1\end{bmatrix}$ et $\begin{bmatrix}1\\ 0\end{bmatrix}$ jouent un rôle spécial. Ces deux vecteurs forment une base pour l'espace vectoriel qui décrit l'état du qubit. Ceci signifie que tout vecteur d'état quantique peut être écrit comme somme de ces vecteurs de base.

Prenons ces deux états quantiques pour correspondre avec les deux états d'un bit classique, à savoir 0 et 1. La convention standard consiste à choisir

$$|0\rangle = \begin{bmatrix}1\\ 0\end{bmatrix} \equiv 0, |1\rangle = \begin{bmatrix}0\\ 1\end{bmatrix} \equiv 1.$$

L'état d'un qubit s'écrit alors

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,.$$

Où α et β sont des coefficients complexes pouvant prendre toutes les valeurs possibles à condition de respecter la relation de normalisation.

Dans le formalisme quantique, α et β représentent des amplitudes de probabilité.

Les qubits peuvent également être représentés à l'aide de la sphère de Bloch. Cette dernière offre un moyen de décrire un état quantique à un qubit sous forme d'un vecteur à valeurs réelles en trois dimensions. Cet aspect est important car il nous permet de visualiser les états à un qubit.

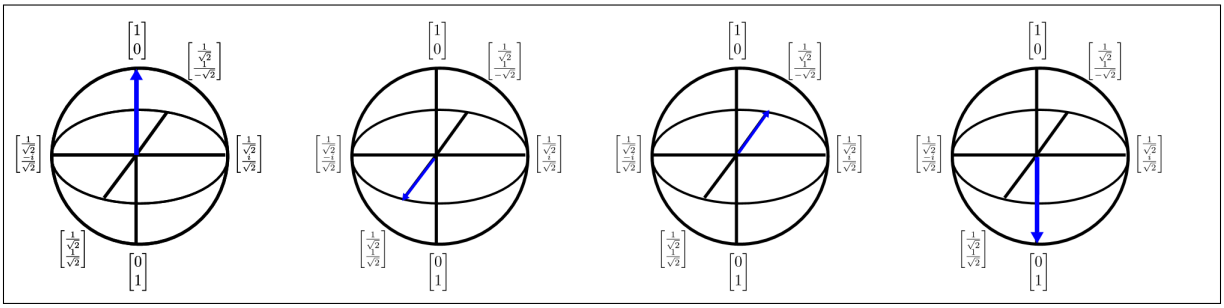

FIGURE 1.1 – Sphère de Bloch [5].

La Figure 1.1 illustre la sphère de Bloch, où les flèches indiquent la direction du vecteur d'état quantique et chaque transformation de la flèche peut être considérée comme une rotation autour de l'un des axes cardinaux.

1.3.2 Matrice de densité

Dans certains cas, un système quantique donné peut être dans un état $|\varphi_1\rangle$ avec une probabilité p_1 et dans un état $|\varphi_2\rangle$ avec une probabilité p_2. Il ne s'agit pas ici d'une superposition des états $|\varphi_1\rangle$ et $|\varphi_2\rangle$. Un formalise permet de décrire les systèmes dont les états potentiels suivent une distribution de probabilité : les matrices de densité [17].

Pour un état $|\varphi\rangle$, la matrice de densité associée est

$$\rho = |\varphi\rangle\langle\varphi|$$

Exemple :

Nous avons ces troit états :

- $|\psi\rangle_1 = |0\rangle$
- $|\psi\rangle_2 = |1\rangle$
- $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Leurs matrices de densité sont :

- $|\psi\rangle\langle\psi|_1 = |0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$

- $|\psi\rangle\langle\psi|_2 = |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$
- $|\psi\rangle\langle\psi| = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$

1.3.3 Mesure d'un qubit

Une mesure correspond à l'idée informelle d'observation d'un qubit, ce qui ramène immédiatement l'état quantique à l'un des deux états classiques $|0\rangle$ ou $|1\rangle$.

Quand un qubit donné par le vecteur d'état quantique $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ est mesuré, nous obtenons le résultat 0 avec la probabilité $|\alpha|^2$ et le résultat 1 avec la probabilité $|\beta|^2$ [5].

Si le résultat est 0, alors le nouvel état du qubit est $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$.

Sinon, son état est $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$.

La somme de ces probabilités $|\alpha|^2 + |\beta|^2 = 1$ en raison de la condition de normalisation.

1.3.4 Portes logiques quantiques

Dans cette section, nous décrivons quelques portes quantiques élémentaires fréquemment utilisées pour le traitement de l'information quantique. Contrairement à de nombreuses portes logiques classiques, les portes logiques quantique sont « réversibles ».

1.3.4.1 Portes à un seul qubit

Dans ce qui suit, nous présentons certaines portes logiques qui agissent sur un seul qubit, à savoir l'identité, pauli-X, pauli-Y et pauli-Z [6].

Porte de Hadamard (H)

La porte de Hadamard agit sur un seul qubit. Elle transforme l'état basique $|0\rangle$ en $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et l'état $|1\rangle$ en $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, ce qui signifie que la mesure aura la même probabilité de donner 1 ou 0 (c'est-à-dire crée une superposition). Elle est representée par la matrice H telle que

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

Identité

L'identité I agit sur un seul qubit. Elle laisse l'état du qubit sur lequel elle a été utilisée tel qu'il est ; elle ne fait aucune modification. Elle est representée par la matrice I telle que

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

Porte pauli-X (NOT)

La porte pauli-X agit sur un seul qubit. Elle transforme $|0\rangle$ en $|1\rangle$ et $|1\rangle$ en $|0\rangle$. C'est pourquoi elle est parfois appelée *bit-flip*. Elle est representée par la matrice X telle que

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

Porte pauli-Y

La porte pauli-Y agit sur un seul qubit. Elle transforme $|0\rangle$ en $i|1\rangle$ et $|1\rangle$ en $-i|0\rangle$. Elle est representée par la matrice Y telle que

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Porte pauli-Z

La porte pauli-Z agit sur un seul qubit. Elle laisse l'état de base $|0\rangle$ inchangé et transforme $|1\rangle$ en $-|1\rangle$. Elle est parfois appelée phase-flip. Elle est representée par la matrice Z telle que

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

1.3.4.2 Portes à plusieurs qubits

Dans ce qui suit, nous présentons une porte logique quantique qui agit sur plusieurs qubits, à savoir la porte CNOT.

Porte contrôlée NOT (CNOT)

La porte contrôlée CNOT agit sur deux qubits et n'effectue l'opération NOT sur le second qubit que lorsque le premier qubit est $|1\rangle$, sinon elle le laisse inchangé. Elle est representée par la matrice $CNOT$ telle que

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

1.3.5 Principes de base

Nous présentons ici certains principes de base sur lesquels repose l'informatique quantique.

1.3.5.1 Superposition d'états

La superposition est la capacité contre-intuitive d'un objet quantique, comme un électron, à exister simultanément dans plusieurs états différents. Il est littéralement dans ces différents états ; à la fois dans un état et dans un autre, sans faire une moyenne des deux. Une mesure détruira cette superposition, et ce n'est qu'alors que l'on pourra dire qu'il est dans l'état inférieur ou supérieur [2].

1.3.5.2 Intrication quantique

D'un point de vue mathématique, deux états quantiques sont intriqués, s'ils ne peuvent pas être écrits séparément. En d'autres termes, ils sont dits intriqués si on ne peut pas les écrire sous forme d'un produit tensoriel. Dans ce mémoire, nous verrons principalement :

- Les quatre (04) états maximalement intriqués de Bell suivants :

  $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.
  $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.
  $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
  $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

- L'état (01) GHZ et l'état (01) W suivants :

  $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.
  $W = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.

1.3.5.3 Téléportation quantique

La téléportation quantique est un protocole de communication (quantique), qui utilise le phénomène d'intrication quantique pour téléporter l'état quantique d'un système, le faisant disparaître de son point de départ et réapparaître instantanément au point d'arrivée [13].

1.4 Concepts de base de la cryptographie

Dans cette section, nous présentons les concepts de base et les principales techniques de la cryptographie classique, moderne, et quantique.

1.4.1 Définition et terminologie

La cryptographie est l'art de chiffrer. En effet, coder les messages est devenu aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, la cryptographie permet ce dont les civilisations ont besoin depuis qu'elles existent ; le maintien de secrets [4].

Parmi les principaux termes relatifs à la cryptographie nous pouvons citer [8] :

- **Chiffrement :** transformation du message de façon à le rendre incompréhensible.
- **Déchiffrement :** reconstruction du message initial contenu dans le texte chiffré.
- **Décrypter :** c'est déchiffrer le message original sans connaître la clé, c'est-à-dire ; en cassant le chiffrement.
- **Texte en clair :** message à chiffrer.
- **Texte chiffré :** aussi appelé cryptogramme, il s'agit du résultat du chiffrement.

1.4.2 Objectifs de la cryptographie

L'objectif fondamental de la cryptographie est de respecter et d'assurer les contraintes de sécurité suivantes [21] :

- **Confidentialité :** assurer que seul le destinataire puisse lire le message en le rendant illisible par d'autres.
- **Authentification :** il doit être possible pour le récepteur du message de garantir son origine. Une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre.
- **Intégrité :** le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant sa transmission. Une tierce personne ne doit pas pouvoir substituer un message légitime (ayant pour origine l'émetteur) par un message frauduleux.
- **Non répudiation :** un émetteur ne doit pas pouvoir nier l'envoi d'un message.

1.4.3 Principales techniques de cryptographie

La cryptographie a progressé au fil des siècles en parallèle avec l'évolution de l'être humain pour pouvoir garantir la protection contre la curiosité et la malveillance des tiers inconnus qui veulent s'acquérir une information jugée confidentielle.

Nous pouvons classer les techniques cryptographiques apparues au fil des siècles en trois (03) grandes catégories présentées dans la Figure 1.2 et décrites dans les sections suivantes.

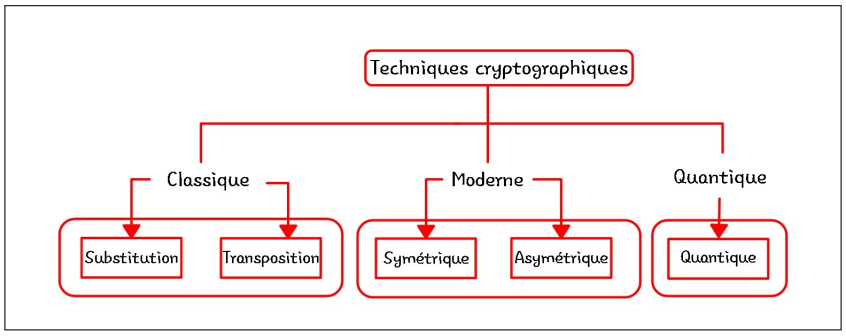

FIGURE 1.2 – Techniques principales de cryptographie.

1.4.3.1 Cryptographie classique

La cryptographie classique décrit la période avant les ordinateurs. Elle traite des systèmes reposant sur des lettres et des caractères d'une langue. Certaines techniques de cryptage utilisées remplacent les caractères par d'autres caractères et les transposent dans un ordre différent, nous décrivons certaines de ces techniques dans ce qui suit.

Chiffrement par substitution

La substitution consiste à effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair. Le destinataire légitime du message applique la dérivée inverse au texte chiffré pour recouvrer le message initial [23]. Le premier système de chiffrement par substitution communément admis par l'Histoire est le chiffre de César, qui utilise le principe de décalage cyclique de l'alphabet.

Soit l'alphabet latin de 26 lettres (de A à Z). Un message $M = l_1 l_2 \cdots l_n$ est chiffré en remplaçant chaque lettre l_i par la lettre c_i obtenue par décalage cyclique, par exemple, de 3 positions dans l'alphabet. Dans ce cas, la lettre A sera remplacée par la lettre D, la lettre Z par C, etc. On peut généraliser ce principe avec un décalage de k positions, où $k = \{1, 2, 3, \cdots, 26\}$. Le paramètre k est alors considéré comme la clé secrète. La Figure 1.3 illustre un exemple du chiffrement de César.

Ce système est facile à casser en force brute (i.e., en essayant toutes les clés possibles) car l'espace des clés est très réduit ; ici, il n'y a que 26 clés possibles. Il suffit alors de tester les 26 possibilités jusqu'à trouver un texte intelligible.

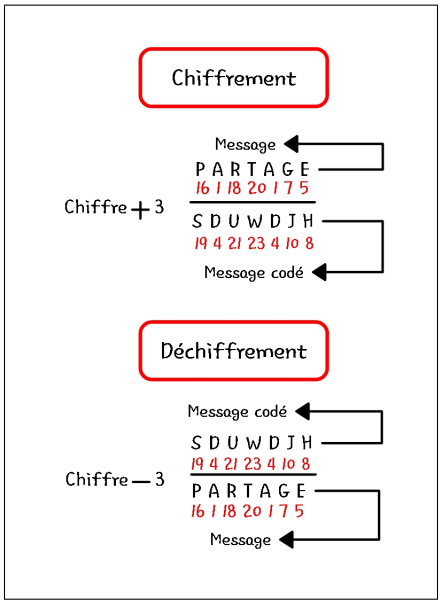

FIGURE 1.3 – Exemple de chiffrement de César.

Chiffrement par transposition

Avec le principe de la transposition, toutes les lettres du message sont présentes mais dans un ordre différent. Elle utilise le principe mathématique des permutations [16]. Une transposition rectangulaire consiste à écrire le message dans une grille rectangulaire, puis à arranger les colonnes de cette grille selon un mot de passe donné, où le rang des lettres dans l'alphabet donne l'agencement des colonnes.

La Figure 1.4 illustre un exemple de chiffrement par transposition rectangulaire. Dans cet exemple, le message en clair « PROTOCOLE DE PARTAGE QUANTIQUE DE SECRET » est chiffré par transposition avec le mot clé « CLAIR ».
Pour effectuer le chiffrement par transposition rectangulaire représenter dans la figure 1.4 nous avons procéder comme suite :

— Nous avons remplie la première ligne avec les lettres du mot-clé « CLAIR » que nous avons choisie.
— Dans la deuxième ligne nous avons mit les numéros qui sont associés aux lettres du mot-clé et qui représente leurs rangs.
— Puis nous avons compléter le tableau en le remplissant avec les lettres de notre message à chiffrer. On a écrit sur chaque ligne autant de lettres que de lettres dans le mot-clé.
— Pour finir, nous avons ordonné les colonnes du tableau selon les numéros associés aux lettres du mot-clé du plus grand rang qui est 1 pour la lettre A au dernier rang 5 qui représente la lettre R.

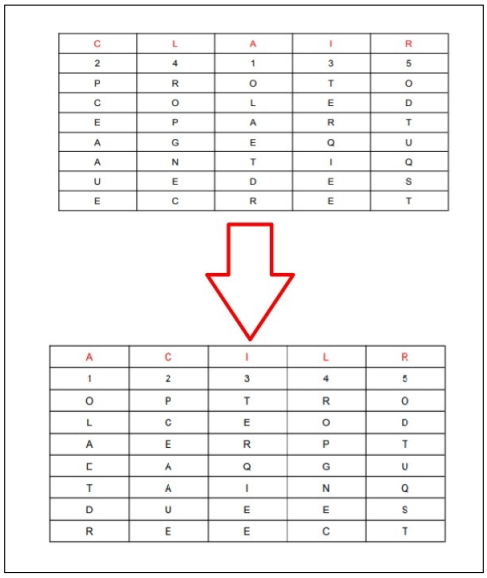

FIGURE 1.4 – Exemple de chiffrement par transposition rectangulaire.

1.4.3.2 Cryptographie moderne

La cryptographie entre dans son ère moderne avec l'arrivée des ordinateurs, celle-ci repose aussi sur les mathématiques avec un privilège bien particulier qui réside dans la facilité que nous procure l'ordinateur pour l'utilisation des principes mathématiques les plus complexes, et qui vont permettre le renforcement de la protection avec des techniques plus efficaces. La cryptographie moderne peut être classée en deux variantes distinctes que nous définissons dans ce qui suit.

Cryptographie symétrique

Dans la cryptographie symétrique, aussi appelée *cryptographie à clé secrète*, deux utilisateurs Alice et Bob souhaitent échanger des informations sur un canal non sécurisé. Leur vecteur de communication peut être « écouté » par Eve, un attaquant. Comme Alice et Bob ne veulent pas divulguer leurs informations à des tiers, la cryptographie symétrique leur offre la possibilité de chiffrer et déchiffrer leur communication. Cependant, ils doivent partager un secret commun (la clé) sur le quel reposera la sécurité de cette technique. Celle clé secrète peut être échangée sur un canal de confiance ou être connue à l'avance [25].

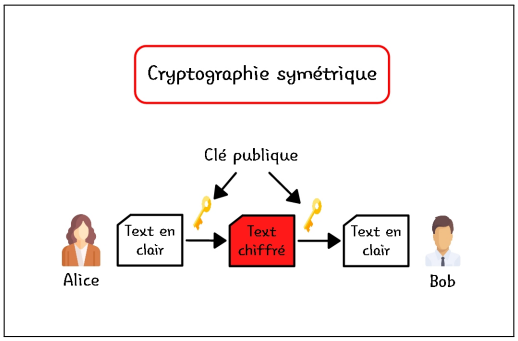

FIGURE 1.5 – Chiffrement symétrique.

Cryptographie asymétrique

Avec la cryptographie asymétrique, les clés de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre. On peut donc rendre l'une des deux publique tandis que l'autre reste privée. C'est pourquoi on parle de *chiffrement à clé publique*. Si la clé publique sert au chiffrement, alors tout le monde peut chiffrer un message que seul le propriétaire de la clé privée correspondante pourra déchiffrer. On assure ainsi la confidentialité des communications. Certains algorithmes permettent d'utiliser la clé privée pour chiffrer. Dans ce cas, n'importe qui pourra déchiffrer mais seul le détenteur de la clé privée peut chiffrer [19].

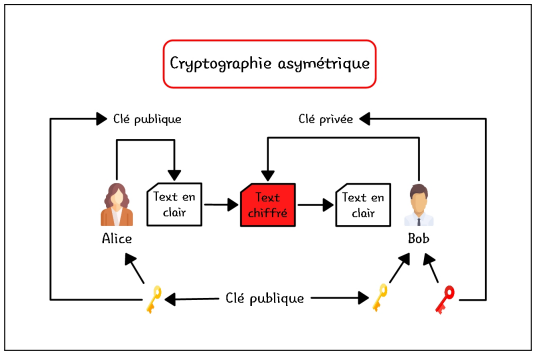

FIGURE 1.6 – Chiffrement asymétrique.

1.4.3.3 Cryptographie quantique

La cryptographie quantique, plus correctement nommée *distribution quantique de clés*, désigne un ensemble de protocoles permettant de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois et aux propriétés de la mécanique quantique. Utilisée dans un algorithme de chiffrement symétrique afin de chiffrer et déchiffrer des données confidentielles, la cryptographie quantique permet non seulement de démasquer toute tentative d'espionnage

grâce aux propriétés de la mécanique quantique, mais également de réduire la quantité d'informations détenue par un éventuel espion à un niveau arbitrairement bas [11].

Comme nous avons pu le voir précédemment, les différentes techniques de cryptographie classique et moderne reposent principalement sur des problèmes mathématiques difficiles à résoudre. C'est là donc où réside l'inconvénient majeur de ces techniques ; une découverte mathématique mènera à la démolition de l'efficacité de ces techniques, tandis que la cryptographie quantique se base sur des principes physiques de la mécanique quantique. En effet, à ce jour aucune découverte technologique ne peut contredire les principes de la physique quantique.

1.5 Partage de secret

Le partage de secret (SS - *Secret Sharing*) est une primitive cryptographique regroupant plusieurs participants dont l'un d'eux est détenteur d'un secret qu'il souhaite partager avec le reste des participants. Dans de tels protocoles, le détenteur attribue à chacun des participants des données spécifiques. Une fois le partage effectué, certains ensembles de participants peuvent reconstruire le secret en mettant en commun leurs données, alors que d'autres n'ont aucun moyen d'y arriver.

1.5.1 Partage de secret classique

Dans un protocole de partage de secret classique (CSS - *Classical Secret Sharing*), on souhaite partager un secret entre des personnes participant au protocole. Le principe est de ne rendre le secret visible à aucun membre participant seul. Pour que le secret soit révélé, les participants doivent au moins être k à mettre leurs données en commun. À ce moment-là, la reconstruction du secret devient une tâche facile. Dans le cas contraire, le secret est complètement impossible à déterminer, dans la mesure où toutes les valeurs possibles sont équiprobables.

Prenons un exemple élémentaire dans lequel cinq (05) personnes participent au protocole. Les participants sont le détenteur du secret D et les quatre participants $P1$, $P2$, $P3$ et $P4$ avec lesquels le détenteur veut partager son secret. Le détenteur détient un secret (s) qu'il souhaite partager avec les quatre participants. Pour cela, il prépare des bits aléatoires a et $a^{'}$ inconnus des autres participants a priori. Il donne ensuite aux quatre participants un bit d'information calculé de la manière suivante :

— D : s.
— P1 : $s \oplus a^{'}$.
— P2 : $a \oplus a^{'}$.
— P3 : $s \oplus a$.
— P4 : a.

On peut constater ici qu'aucun participant à lui seul ne peut reconstruire le secret final. Cependant, comme nous pouvons le remarquer la collaboration des deux participants $P3$ et $P4$ peut mener à la reconstruction du secret s'ils additionnent leurs bits, de même pour l'ensemble des participants $\{P1, P2, P4\}$. Par ailleurs, si d'autres participants décident de collaborer, ils ne pourront pas reconstruire le secret tels que $\{P1, P2\}$ et $\{P1, P3\}$.

1.5.2 Partage de secret quantique

Dans un protocole de partage de secret quantique (QSS - *Quantum Secret Sharing*), le but à atteindre reste inchangé ; permettre le partage d'un secret entre les différentes personnes participant au protocole. Ce secret peut être classique ou quantique. Étant une branche importante de la cryptographie quantique, le partage de secret quantique s'appuie lui aussi sur les phénomènes de la mécanique quantique pour fournir une protection du partage du secret plus robuste, comparée aux protocoles de partage de secret classique.

Avec le principe de non-clonage, faire la copie du secret s'avère impossible. Contrairement à un bit, un qubit ne peut pas être copié car il faudrait d'abord le mesurer. Or, la mesure d'un qubit qui est en état de superposition entraînera une perturbation qu'il lui fera perdre son aspect d'origine. Ceci pouvant mener à la perte de la possibilité de découverte de l'état d'origine d'une part, et de la détection d'une quelconque tentative d'appropriation du secret, d'autre part.

1.6 Conclusion

Dans ce premier chapitre, nous avons en premier lieu présenté des généralités sur le domaine de l'informatique en définissant ses deux variantes et en faisant la comparaison entre elles. Nous avons ensuite évoqué des concepts de base du domaine de la cryptographie. Enfin, nous avons abordé un sous-domaine spécifique de la cryptographie sur lequel repose la problématique de notre projet, il s'agit du partage de secret que nous avons défini et dont nous avons présenté les deux types, à savoir classique et quantique. La lecture de ce chapitre permet d'acquérir toutes les informations requises pour la compréhension du chapitre suivant qui consiste en un état de l'art des protocoles de partage de secret quantique existants.

Chapitre 2

État de l'art sur les protocoles de partage de secret quantique

2.1 Introduction

Jusqu'à présent, plusieurs protocoles quantiques ont été proposés dans le but commun d'assurer un partage de secret sécurisé. Dans ce chapitre, nous donnerons un aperçu de différents protocoles quantiques de partage de secret existants. Nous commencerons donc par classer ces protocoles, puis nous décrirons chaque protocole analysé et terminerons enfin par une synthèse comparative de ces protocoles.

2.2 Classification et description des protocoles analysés

Dans cette section, nous décrivons les protocoles étudiés et les classifions en suivant le type de secret partagé ; déterministe prédéfini par les utilisateurs ou non-déterministe généré aléatoirement pour faire office de clé secrète partagée.

2.2.1 Protocoles déterministes

Nous analysons dans cette catégorie trois (03) protocoles proposés par Choudhury et al. [12], Musanna et Kumar [20], et Wang et al. [26].

2.2.1.1 Multilayer quantum secret sharing based on GHZ state and generalized Bell basis measurement in multiparty agents

Ce protocole de Wang et al. [26] est un protocole de partage de secret quantique multi-couches basé sur l'utilisation des états quantiques GHZ et sur le processus de mesure généralisée dans la base de Bell. L'objectif du protocole est le partage d'un secret appartenant à Alice avec d'autres agents du réseau. La transmission se fait couche par couche en partant de la couche racine Alice vers les agents des autres couches. Ce n'est que lorsque tous les agents de la dernière couche coopèrent ensemble que le secret peut être récupéré.

Si Alice a pour intention de partager un qubit avec 3 agents, alors les étapes à suivre du protocole sont les suivantes :

1. Alice prépare d'abord 4 particules dans un état GHZ maximalement intriqué ; $|\psi\rangle_{1\,234} = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)_{1234}$

2. Alice envoie 3 de ces particules aux trois agents pour configurer le canal quantique ;

3. Alice effectue une mesure dans la base de Bell de l'état du qubit qu'elle a gardé puis envoie le résultat par le canal classique aux agents. Après avoir reçu le résultat, les agents effectuent chacun des opérations unitaires (I/X/Y/Z) sur chacun des qubits qu'ils ont reçu de Alice. Un état quantique de 3 qubits partagé entre les trois agents en est engendré. Les trois agents doivent coopérer pour effectuer une mesure et récupérer l'information complète.

4. Alice désigne un agent pour récupérer l'état quantique. De ce fait, les autres agents devraient chacun effectuer une mesure dans la base $|X^{\pm}\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ sur leur propre qubit. Puis, ils communiqueront les résultats de leur mesure par le canal classique à l'agent désigné. Après avoir reçu le résultat de la mesure, l'agent désigné peut récupérer les informations d'origine en appliquant une transformation unitaire appropriée sur sa particule.

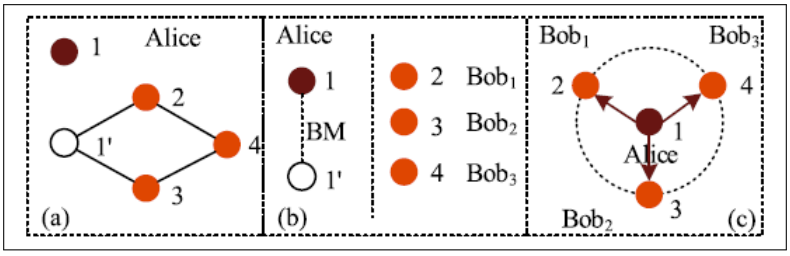

FIGURE 2.1 – La distribution dans la première couche [26].

Si Alice souhaite partager le secret avec des agents d'une deuxième couche, les trois agents de la première couche ne doivent pas retrouver l'état quantique sous peine de perdre l'information. La distribution avec une deuxième couche composé de neuf (09) agents se passe alors comme suit :

1. Les 3 agents de la première couche doivent chacun préparer quatre qubits dans un état GHZ maximalement intriqué.

2. L'étape de la configuration du canal quantique se passe de la même manière que précédemment. La démarche à suivre dans cette étape est que chaque agent de la première couche envoie une particule à des agents de la deuxième couche ; l'agent 1

de la première couche envoie respectivement les particules 5, 6 et 7 aux agents 1, 2 et 3 de la deuxième couche. L'agent 2 de la première couche envoie respectivement les particules 8, 9 et 10 aux agents 4, 5 et 6 de la deuxième couche. Et finalement, l'agent 3 de la première couche envoie respectivement les particules 11, 12 et 13 aux agents 7, 8 et 9 de la deuxième couche.

3. Les agents de la première couche effectueront une mesure dans la base de Bell de la particle qu'ils ont gardé et envoient le résultat par un canal classsique aux agents de la deuxième couche. Après que les agents de la deuxième couche aient reçu le résultat, ils effecturont une transformation unitaire pour pouvoir se procurer l'information complète. Seuls les agents de la deuxième couche peuvent reconstruire le secret en coopérant.

4. Alice désigne un agent de la deuxième couche pour récupérer l'état quantique. De ce fait, les autres agents devraient chacun effectuer une mesure dans la base $|X^{\pm}\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ sur leur propre qubit. Ils communiqueront ensuite les résultats de leur mesure par le canal classique à l'agent désigné. Après avoir reçu le résultat de la mesure, l'agent désigné peut récupérer les informations d'origine en appliquant une transformation unitaire appropriée sur sa particule.

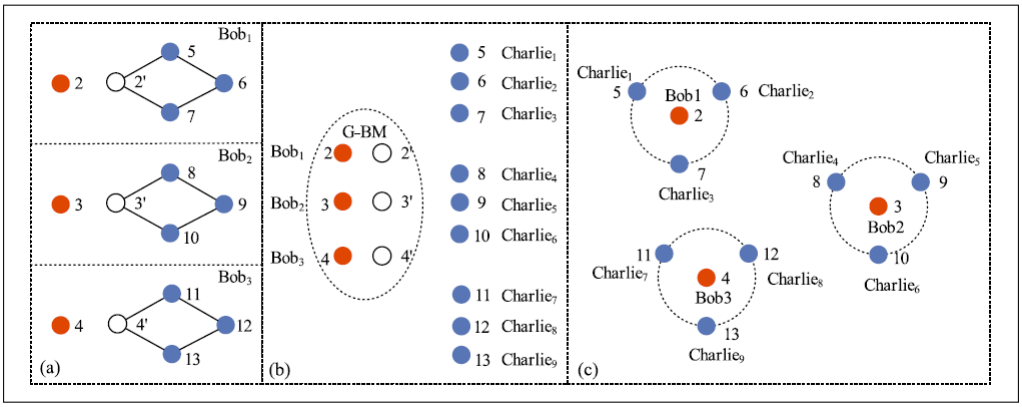

FIGURE 2.2 – La distribution dans la deuxième couche [26].

Afin que davantage d'agents puissent partager les informations quantiques, Alice doit continuer à distribuer dans la couche supérieure. Les agents de la seconde couche ne doivent pas retrouver l'état quantique en raison de son irréversibilité, et la démarche à suivre est la même que celle définie auparavant.

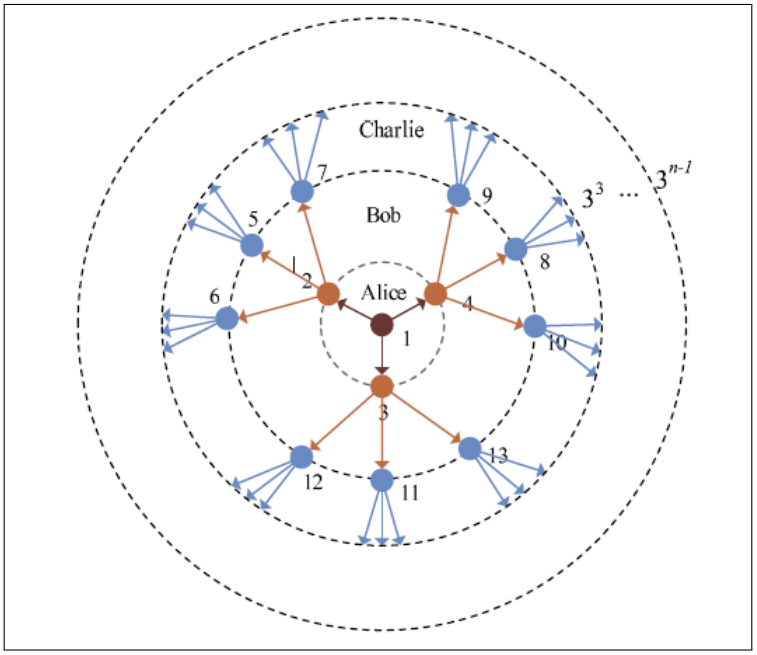

FIGURE 2.3 – Distribution dans n couches [26].

Avantages et inconvénients du protocole

- Il permet une distribution de secret avec un nombre conséquent d'agents ;
- Il pourrait être utilisé dans un réseau sans fil afin de garantir la sécurité de la transmission des informations ;
- Une diffusion des informations dans le réseau sans fil rapide ;
- La complexité de la préparation d'un état GHZ avec plus de particules présente un obstacle pour le protocole.

2.2.1.2 A novel three-party quantum secret sharing scheme based on Bell state sequential measurements with application in quantum image sharing

Ce deuxième protocole proposé par Musanna et Kumar [20] est un protocole de partage quantique de secret entre 3 utilisateurs, pouvant être généralisé à n utilisateurs, où tous les participants doivent s'entendre pour reconstruire le secret original. Pour concevoir ce protocole, les états de Bell et les oppérateurs de Pauli ont été utilisés.

Dans ce protocole, quand un détenteur de secret (D) souhaite le partager avec d'autres participants (P1, P2, P3) il doit procéder comme suit :

1. Le détenteur du secret (D) génère un état produit avec l'un des quatre états de Bell possibles et les partage avec les trois participants P1, P2 et P3 tel que pour chaque participant, une paire de qubits non intriqués (2 qubits de deux paires différentes de

qubits intriqués) est attribuée.

$$|\psi\rangle = (\frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2))(\frac{1}{\sqrt{2}}(|0\rangle_3 |0\rangle_4 + |1\rangle_3 |1\rangle_4))(\frac{1}{\sqrt{2}}(|0\rangle_5 |0\rangle_6 + |1\rangle_5 |1\rangle_6))$$

Supposons que P1 obtienne les qubits 1 et 4, P2 obtienne les qubits 2 et 6, P3 obtienne les qubits 3 et 5. Cette allocation peut être n'importe quelle autre combinaison à condition que chaque partie ait une part de l'autre particule intriquée.

2. Avant d'envoyer les particules aux trois participants, le détenteur de secret (D) modifie d'abord chacune des particules à envoyer aux participants en soumettant l'une des particules de la paire à une porte logique (I/X/Y/Z). Il envoie les qubits au premier participant P1, qui fera des mesures dans la base de Bell sur ses particules.

3. Le détenteur de secret (D) peut employer les autres portes sur les particules du premier participant P1. Au final, pour chaque porte (opération), les mesures que peut faire le premier participant P1 et les états réduits résultants peuvent être répertoriés dans un tableau contenant les opérations unitaires et les résultats de mesure correspondants .

4. Le détenteur de secret (D) annonce de manière publique l'état du produit créé et quel qubit à été transformé.

5. Le premier participant P1 annonce quelle mesure de Bell a été effectuée sur ses qubits.

6. Les deux autres participants P2 et P3 effectuent des mesures sur leurs qubits respectifs et s'entendent pour retrouver l'opération effectuée par le 1er participant P1 dans le tableau obtenue précédemment.

De cette manière, les trois participants P1, P2 et P3 conservent leurs parts du secrets qui seront utilisés lors de la procédure de reconstruction du secret. La reconstruction du secret se fait alors de la manière suivante :

Outre les informations obtenues précédemment, les participants P2 et P3 annoncent leurs mesures publiquement. Ils s'assureront ensuite que leurs qubits n'ont pas été falsifiés et en utilisant les résultats de mesure du premier participant P1 et l'annoncement du détenteur du secret (D) de la transformation faite au qubit, ils déduiront l'état actuel.

En utilisant les informations concernant l'état que le détenteur du secret (D) a créé, ils déduiront quelle opération a agi sur le qubit modifié. Finalement, ils pourront acquérir le

secret original.

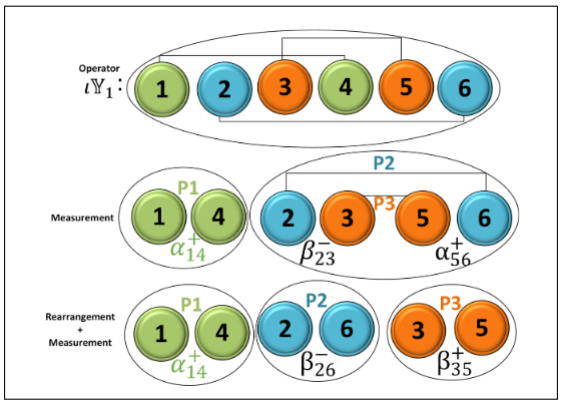

FIGURE 2.4 – Le protocole proposé dans [20].

Avantages et inconvénients du protocole

- La sécurité du protocole contre un adversaire est assez substantielle ;
- L'état de la paire EPR n'est connu que de son générateur, ce qui augmente la sécurité du protocole ;
- Le protocole proposé peut fournir un partage parfait du secret visuel(les secrets cachés dans les images numériques) ;
- La reconstruction du secret n'est pas possible s'il y a des manipulations par un adversaire ;
- L'apparition d'erreurs lors de la transmission du secret quantique sur de longues distances et à cause des canaux bruyants.

2.2.1.3 Asymmetric bidirectional quantum state exchange between Alice and Bob through a third party

Ce troisième protocole est un protocole de téléportation bidirectionnel asymétrique contrôlé proposé par Choudhury et al. [12] dans le but de permettre l'échange d'états quantiques entre deux parties qui se trouvent éloignées l'une de l'autre, et ce avec l'aide d'une tierce personne jouant le rôle du contrôleur. Un canal intriqué multiqubit multipartie et deux états, l'un étant un état W généralisé à trois qubits, et l'autre, un état intriqué arbitraire à deux qubits, ont été utilisés. Ainsi, il est supposé que deux parties, à savoir, Alice et Bob, détiennent respectivement un état $W = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ à 3 qubits et un état intriqué arbitraire à deux qubits. Le protocole est alors exécuté de la manière suivante :

1. Alice, Bob et le contrôleur Charlie partagent un état de cluster de 10 qubits comme canal de partage quantique, où chacun des trois possède des particules du canal ;

2. Seize états orthonormés linéairement indépendants sont considérés pour des particules appartenant à Alice, de même pour Bob.

$$\begin{pmatrix} |\xi_1\rangle \\ |\xi_2\rangle \\ |\xi_3\rangle \\ |\xi_4\rangle \end{pmatrix} = X \begin{pmatrix} |00000\rangle \\ |00101\rangle \\ |01010\rangle \\ |10011\rangle \end{pmatrix}_{a_1a_2a_3A_3A_4} \quad \begin{pmatrix} |\xi_5\rangle \\ |\xi_6\rangle \\ |\xi_7\rangle \\ |\xi_8\rangle \end{pmatrix} = X \begin{pmatrix} |00001\rangle \\ |00100\rangle \\ |01011\rangle \\ |10010\rangle \end{pmatrix}_{a_1a_2a_3A_3A_4}$$

$$\begin{pmatrix} |\xi_9\rangle \\ |\xi_{10}\rangle \\ |\xi_{11}\rangle \\ |\xi_{12}\rangle \end{pmatrix} = X \begin{pmatrix} |00010\rangle \\ |00111\rangle \\ |01000\rangle \\ |10001\rangle \end{pmatrix}_{a_1a_2a_3A_3A_4} \quad \begin{pmatrix} |\xi_{13}\rangle \\ |\xi_{14}\rangle \\ |\xi_{15}\rangle \\ |\xi_{16}\rangle \end{pmatrix} = X \begin{pmatrix} |00011\rangle \\ |00110\rangle \\ |01001\rangle \\ |10000\rangle \end{pmatrix}_{a_1a_2a_3A_3A_4}$$

FIGURE 2.5 – Les Seize états orthonormés [12].

3. Alice effectue une mesure sur les états de ses qubits dans n'importe quelle de ces 16 bases, Bob fera la même chose avec ses états, tel que les mesures des deux participants sont indépendantes l'une de l'autre.

4. Alice et Bob envoient leurs résultats de mesure au contrôleur Charlie. Ce dernier interprète de son côté son résultat de mesure sur son seul qubit et transmet à Bob le résultat de sa mesure avec le résultat qu'il a obtenu d'Alice. Il transmet également à Alice son résultat de mesure avec le résultat qu'il a obtenu de Bob.

5. Le protocole est achevé de la manière suivante : en se basant sur les informations transmises, Alice et Bob effectuent des opérations unitaires appropriées sur les états en leurs possessions pour pouvoir récupérer l'état d'origine.

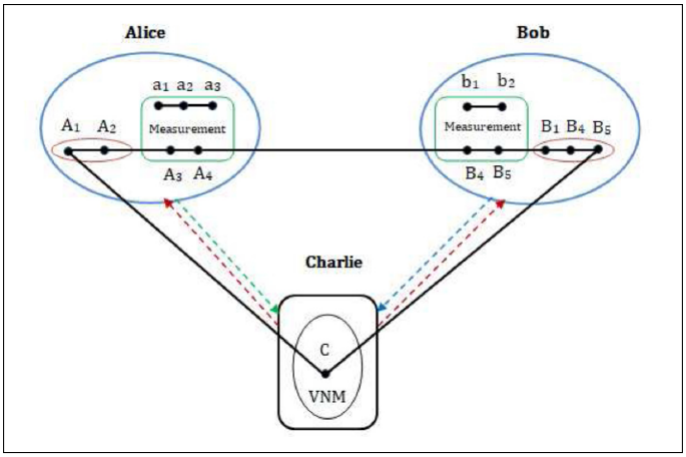

FIGURE 2.6 – Le protocole proposé dans [12].

Avantages et inconvénients du protocole

- Le protocole ne comporte théoriquement aucun cas d'échec ;
- L'échange bidirectionnel se produit avec une fidélité unitaire aux deux extrémités ;
- La difficulté de préparer des états intriqués représente un obstacle dans ce protocole ;
- Les problèmes associés au transfert d'états quantiques comme les erreurs induites par la mesure et l'effet des paramètres expérimentaux ;
- Le protocole consomme un taux élevé de qubits. Cependant, son efficacité est bien plus élevée aux autres protocoles avec lesquels il a été comparé.

2.2.2 Protocoles non-déterministes

Nous analysons dans cette seconde catégorie trois (03) autres protocoles proposés par Deng et al. [15], Sun et al. [24], et Zhu et al. [27].

2.2.2.1 An efficient quantum secret sharing scheme with EPR pairs

Le protocole proposé par Deng et al. [15] utilise l'idée du codage dense, la réorganisation de l'ordre des paires de qubits dans un état EPR, et deux canaux classique et quantique pour le partage de l'information tout en garantissant la sécurité de l'échange contre les oreilles indiscrètes qui veulent acquérir l'information. Trois (03) acteurs participent à ce protocole, à savoir, Alice, Bob et Charlie.

Le protocole se déroule selon les cinq (05) étapes suivantes :

— **Étape 1 :** Alice prépare au hasard une séquence de paires EPR dans l'un des états de Bell. Puis, elle enregistre les états des paires EPR. Ces paires seront divisées en groupes, où chaque groupe contient quatre paires EPR.

— **Étape 2 :** Alice prend chaque particule à partir d'une paire EPR dans un groupe et les envoie à Bob dans leur ordre original à travers le canal AB. Elle effectue ensuite pour les 4 particules restantes un réarrangement d'ordre avant de les envoyer à Charlie via le canal AC.

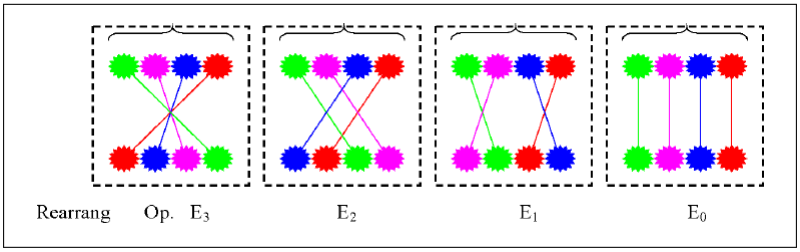

FIGURE 2.7 – Les quatre opération de réarangenment possibles [15].

— **Étape 3 :** Après avoir reçu les particules, Bob et Charlie choisissent aléatoirement et indépendamment l'un des deux modes ; vérification ou codage. Enfin, après avoir effectué les mesures, ils renvoient les particules à Alice.

— **Étape 4 :** Après avoir reçu les particules de Bob et de Charlie, Alice annule l'opération de réarrangement d'ordre qu'elle a effectuée pour récupérer la correspondance correcte des paires EPR, et ce, pour celles qui ne sont pas choisies pour la vérification d'intrusion. Elle effectue ensuite une mesure dans la base de Bell pour chaque paire, de telle sorte qu'elle connaît l'état après les opérations combinées de Bob et Charlie, et qu'elle puisse vérifier qu'il n'y a pas eu d'espionnage.

— **Étape 5 :** Alice annonce publiquement l'opération de réarrangement de l'ordre pour chaque groupe et les particules qui ont été choisies pour la vérification d'intrusion. Avec ces informations, Bob et Charlie obtiennent la correspondance correcte de leurs particules. L'opération combinée de Bob et Charlie est la clé qu'Alice souhaite qu'ils partagent, et qu'ils utiliseront lorsqu'ils travailleront ensemble comme clé secrète partagée.

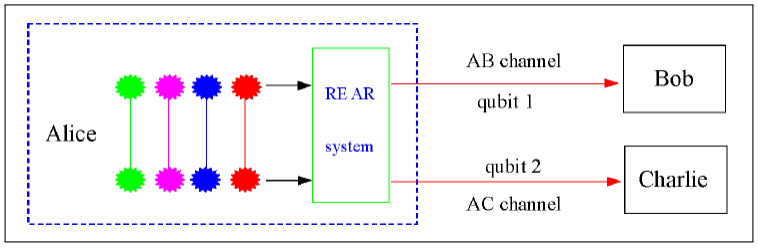

FIGURE 2.8 – Illustration du protocole proposé dans [15].

Avantages et inconvénients du protocole

- La communication classique est réduite, ce qui entraîne un renforcement de la sécurité ;
- Il est efficace de par son determinisme, puisque presque toutes les paires EPR peuvent être utilisées pour le partage du secret, sauf celles choisies pour la détection d'intrusion ;
- Deux bits d'information sont transportés par chaque paire EPR, et ce, pour chaque cycle de communication réussi.

2.2.2.2 Two new Controlled not Gate Based Quantum Secret Sharing Protocols without Entanglement Attenuation

Deux protocoles sont proposés par Zhu et al. [27] pour le partage de l'information avec la garantie de la sécurité de la transmission entre les differentes parties qui y participent. Dans les deux protocoles des paires EPR et la porte contrôlée NOT (CNOT) ont été utilisées.

Protocole 1

Pour le premier protocole proposé, trois (03) parties y participent, à savoir, Trent, Alice et Bob tel que le Boss Trent veut partager son secret avec ses deux agents Alice et Bob, suivant les six (06) étapes du protocole :

- **Étape 1 :** Trent prépare N paires EPR qui sont toutes dans l'état de Bell $|\phi^+\rangle_{AB} = 1/\sqrt{2}(|00\rangle + |11\rangle)$. Il prend la première et la deuxième particule de chaque paire pour former des séquences S_A et S_B ensuite, il prépare deux séquences de photons comme leurres dans lesquelles chaque photon est aléatoirement dans l'une des bases Base-Z $\{|0\rangle, |1\rangle\}$ ou Base-X $\{|+\rangle, |-\rangle\}$ tel que

  $$|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$$
  $$|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$$

  Puis, il les insère au hasard dans S_A et (S_B) pour former S'_A et S'_B, avant de les envoyer à Bob et Alice, respectivement.

- **Étape 2 :** Trent s'assure que Alice et Bob aient bien reçu les éléments envoyés à travers un canal classique, ensuite il annonce les positions et les bases des photons leurres. De leurs côtés, Alice et Bob prennent les photons leurres et mesurenent leurs états, puis annoncent les résultats obtenus. Trent calcule le taux d'erreur, s'il dépasse le seuil prédéterminé alors ils arrêtent le protocole et recommencent depuis le début. Sinon, Alice et Bob préparent une séquence de photons S_a et (S_b), respectivement, dans lequelles chaque photon est aléatoirement dans l'un des états $|0\rangle$ ou $|1\rangle$. Chacun d'eux prend ensuite le photon dans S_a et S_b comme qubit cible et ceux dans S_A et S_B comme qubit de contrôle pour effectuer l'opération CNOT, puis préparent des photons leurres et les insèrent dans S_a et S_b pour qu'ils forment S'_a et S'_b, et les envoient à Trent.

- **Étape 3 :** Alice et Bob s'assurent que Trent ait bien reçu les éléments envoyés, ils annoncent ensuite les positions et les bases des photons leurres en S'_a et S'_b. De son côté, Trent capte les photons leurres dans la séquence correspondante et effectue des mesures sur eux, puis annonce les résultats obtenus. De leur côté, Alice et Bob calculent les taux d'erreur correspondants. Si l'un des deux débits dépasse le seuil prédéterminé alors ils arrêtent le protocole et reviennent à la première étape.

- **Étape 4 :** Alice et Bob effectuent une mesure dans la base X sur les photons correspondants dans S_A et S_B, respectivement. Trent mesure les paires de photons correspondantes dans S_a et S_b danc la base de Bell pour obtenir N ensembles de clés principales à deux bits K_T, tels que les bits correspondants dans K_T sont :

  — 00 si le résultat de la mesure est : $|\phi^+\rangle$;
  — 01 si le résultat de la mesure est : $|\phi^-\rangle$;
  — 10 si le résultat de la mesure est : $|\psi^+\rangle$;
  — 11 si le résultat de la mesure est : $|\psi^-\rangle$.

  où

  $|\phi^-\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$.
  $|\psi^{\pm}\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$.

- **Étape 5 :** Alice et Bob convertissent les états initiaux des photons préparés et les résultats de la mesure dans la base X sur les photons correspondants dans S_A et S_B, respectivement, en N ensembles de clés à deux bits K_A et K_B, où les bits dans K_A et K_B sont :

  — 00 si l'état initial est $|0\rangle$ et le résultat de la mesure $|+\rangle$;
  — 01 si l'état initial est $|0\rangle$ et le résultat de la mesure $|-\rangle$;
  — 10 si l'état initial est $|1\rangle$ et le résultat de la mesure $|+\rangle$;
  — 11 si l'état initial est $|1\rangle$ et le résultat de la mesure $|-\rangle$;

  tels que les trois clés satisfont l'équation suivante : $K_T = K_A \bigoplus K_B$.

- **Étape 6 :** Trent sélectionne suffisamment de bits dans K_T pour le contrôle final. Alice et Bob publient leurs bits correspondants dans un ordre aléatoire. Si le taux d'erreur dépasse une valeur seuil prédéterminée, Trent annonce qu'il faut refaire le protocole. Sinon, Alice et Bob peuvent partager les bits restants, qui peuvent être récupérés en effectuant une opération XOR sur leurs clés restantes ou selon une table qui présente les relations entre la clé principale de Trent et leurs clés.

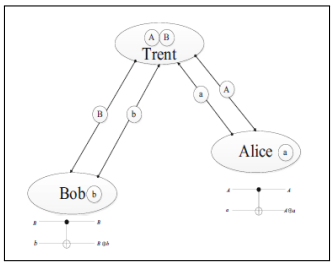

FIGURE 2.9 – Illustration du premier protocole proposé dans [27].

Protocole 2

Quatre (04) parties participent au second protocole, à savoir, Trent, Alice, Charlie et Bob tels que le Boss Trent veut partager son secret avec ses trois agents Alice, Charlie et Bob. Pour ce faire, ils doivent suivre les six (06) étapes décrites ci-après :

- **Étape 1 :** Les procédures sont les mêmes que celles suivies lors de l'étape 1 du Protocole 1, elle diffère dans les destinataires de $S_A^{'}$ et $S_B^{'}$, qui seront respectivement Alice et Charlie au lieu de Alice et Bob.

- **Étape 2 :** Au début Alice et Charlie réalisent les mêmes procédures suivies lors de l'étape 2 du Protocole 1. Arrivé à l'instant où ils doivent préparer une séquence de photons S_a et S_c, respectivement, Alice (Charlie) prend le photon dans S_a (S_c) comme qubit cible et ceux dans S_A (S_B) comme qubit de contrôle pour effectuer l'opération CNOT. Ensuite, Alice (Charlie) prépare des photons leurres puis les insère dans S_a (S_c) pour qu'ils forment $S_a^{'}$ ($S_c^{'}$) et les envoient à Trent et Bob. Alice et Charlie conservent S_A et S_B, respectivement.

- **Étape 3 :** Après qu'Alice et Charlie se soient assurés que Trent et Bob aient bien reçu les éléments envoyés, ils annoncent les positions et les bases des photons leurres en $S_a^{'}$ et $S_c^{'}$, respectivement. De leur côté, Trent et Bob effectuent des mesures sur les photons leurres puis annoncent les résultats. Alice et Charlie calculent ensuite le taux d'erreur. Si l'un des deux taux dépasse le seuil prédéterminé alors ils arrêtent le protocole et recommencent depuis le début.

- **Étape 4 :** Bob prépare une séquence de photon S_b dans laquelle chaque photon est aléatoirement dans l'état $|0\rangle$ ou $|1\rangle$. Il prend chaque photon dans S_b comme qubit cible et le photon dans S_a comme qubit de contrôle pour effectuer l'opération CNOT. Il prépare ensuite des photons leurres puis les insère dans S_b pour former la séquence $S_b^{'}$. Bob envoie alors $S_b^{'}$ à Trent et conserve S_a.

- **Étape 5 :** Après que Bob se soit assuré de la réception de l'élément par Trent, il annonce les positions et les bases de mesure de tous les photons leurres dans la séquence $S_b^{'}$. Trent, de son côté, effectue des mesures sur les photons leurres, puis annonce les résultats. Bob calcule alors le taux d'erreur, s'il dépasse le seuil prédéterminé alors ils arrêtent le protocole et recommencent depuis le début.

- **Étape 6 :** Alice (Bob, Charlie) effectue une mesure dans la base X sur les photons correspondants dans S_A (respectivement, dans S_a et S_B), puis convertit les états initiaux des photons préparés et les résultats de la mesure en N ensembles de clés à deux bits K_A (respectivement, K_B et K_C), où les bits dans K_A (respectivement, dans K_B et K_C) sont :

— 00 si l'état initial est $|0\rangle$ et le résultat de la mesure $|+\rangle$;
— 01 si l'état initial est $|0\rangle$ et le résultat de la mesure $|-\rangle$;
— 10 si l'état initial est $|1\rangle$ et le résultat de la mesure $|+\rangle$;
— 11 si l'état initial est $|1\rangle$ et le résultat de la mesure $|-\rangle$.

Trent mesure les paires de photons correspondantes dans S_b et S_c à l'état de Bell pour obtenir N ensembles de clés principales à deux bits K_T, tel que les bits correspondants dans K_T sont :

— 00 si le résultat de la mesure est : $|\phi^+\rangle$;
— 01 si le résultat de la mesure est : $|\phi^-\rangle$;
— 10 si le résultat de la mesure est : $|\psi^+\rangle$;
— 11 si le résultat de la mesure est : $|\psi^-\rangle$;

tels que les quatre clés satisfont l'équation suivante : $K_T = K_A \bigoplus K_B \bigoplus K_C$.

Pour conclure, Trent sélectionne suffisamment de bits de K_T pour le contrôle final, puis demande à tous les agents de publier leurs bits correspondants dans un ordre aléatoire. Ils calculent ensuite le taux d'erreur, s'il dépasse le seuil prédéterminé alors Trent leur demande de recommencer le protocole. Sinon, Alice, Bob et Charlie partagent les bits restants, qui pourront être récupérés selon l'équation précédente ou selon des tables définies.

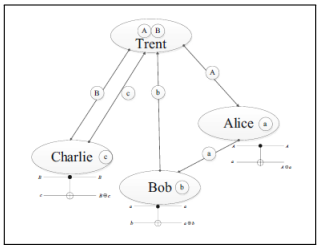

FIGURE 2.10 – Illustration du deuxième protocole proposé dans [27].

Avantages et inconvénients du protocole

- La résolution du problème d'atténuation d'enchevêtrement quantique que rencontrent les agents situés à longue distance puisque chaque photon ne voyage qu'une seule fois ;
- Il garantit une protection contre divers attaques ; les attaques par chevaux de Troie, d'interception-renvoi, par mesure d'enchevêtrement et d'échange d'enchevêtrement ;
- Tous les états intriqués peuvent être utilisés pour le partage final du secret ;
- L'utilisation des photons leurres facilite la détection d'intrusions ;
- Il permet le partage de l'information avec plusieurs participants.

2.2.2.3 Multiparty quantum secret sharing based on Bell measurement

Il s'agit d'un protocole de partage de secret quantique multipartie basé sur la mesure de Bell et proposé par Sun et al. [24]. Dans ce protocole, trois (03) acteurs y participent, à savoir Trent, Alice et Bob, tandis que pour la réalisation du protocole, quatre (04) états de Bell et deux (02) états GHZ ont été utilisés.

Les états utilisés

Les quatre (04) états de Bell :

— $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$.
— $|\phi^-\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$.
— $|\psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$.
— $|\psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$.

Les deux (02) états GHZ :

— $|\phi\rangle = 1/\sqrt{2}(|000\rangle + |111\rangle)$.
— $|\psi\rangle = 1/\sqrt{2}(|001\rangle + |110\rangle)$.

Les différentes étapes du protocole peuvent être résumées comme suit :

- **Étape 1 :** Trent prépare $2n$ états GHZ $\{|\varphi_1\rangle_{TAB}, |\varphi_2\rangle_{TAB}, \ldots, |\varphi_{2n}\rangle_{TAB}\}$ au hasard dans l'un des états $\{|\phi\rangle, |\psi\rangle\}$, où les indices T, A, et B désignent respectivement les trois particules dans chaque état GHZ. Les séquences formées par les trois particules intriquées de chaque état GHZ sont notées respectivement S_T, S_A et S_B.

- **Étape 2 :** Trent prépare deux ensembles de particules pour l'analyse statistique de l'écoute clandestine, qui sont désignés respectivement par D_{TA} et D_{TB}, où les indices TA (respectivement, TB) désigne l'ensemble d'échantillons utilisé pour vérifier la sécurité lorsque la séquence S_A (respectivement, S_B) est transmise de Trent à Alice (respectivement, à Bob). Chaque particule dans TA (respectivement, dans TB) est préparée au hasard dans l'une des bases X ou Z.

  Trent insère ensuite D_{TA} et D_{TB} dans S_A et S_B, respectivement. Chaque particule dans D_{TA} (respectivement, dans D_{TB}) est distribuée dans une position aléatoire de S_A (respectivement, de S_B). La nouvelle séquence est désignée par S_A^d (respectivement, S_B^d), où l'exposant d désigne la séquence avec l'ensemble d'échantillons D_{TA} (respectivement, D_{TB}).

- **Étape 3 :** Trent envoie les séquences S_A^d et S_B^d, respectivement à Alice et Bob, et

conserve la séquence S_T restante.

- **Étape 4 :** Après que Trent se soit assuré via à canal classique que Alice et Bob aient bien reçu les séquences S_A^d et S_B^d, respectivement, il annonce les positions des particules appartenant à D_{TA} (respectivement, D_{TB}) dans la séquence S_A^d (respectivement, S_B^d) et la base de mesure.

  Alice et Bob mesurent alors les particules de l'échantillon dans D_{TA} et D_{TB}, respectivement, selon l'annonce de Trent, puis ils lui partageront les résultats de la mesure. Trent de son côté compare les résultats de mesure annoncés par les agents aux états initiaux des particules dans D_{TA} et D_{TB}, et analyse la sécurité des transmissions. Si l'un des taux d'erreur est supérieur au seuil déterminé par le bruit du canal alors Trent annule le protocole et ils devront redémarrer dès le début. Sinon, ils passeront à l'étape suivante.

- **Étape 5 :** Trent, Alice et Bob mesurent respectivement chaque état de deux particules de la séquence S_T, S_A et S_B dans la base de Bell. Ils transforment ensuite leurs séquences de résultats de mesure en chaînes de bits classiques conformément au schéma de codage suivant :

$$|\phi^+\rangle \Rightarrow 00, |\phi^-\rangle \Rightarrow 01, |\psi^+\rangle \Rightarrow 10, |\psi^-\rangle \Rightarrow 11,$$

  où ils désignent respectivement ces chaînes de bits par K_T, K_A et K_B.

- **Étape 6 :** Trent génère la clé commune K'_T, qui satisfait la relation : $K'_T = K_A \oplus K_B$.

  Par conséquent, K_A et K_B peuvent être considérées comme clés partagées de Alice et de Bob. Trent peut adopter le protocole one-time pad pour crypter son secret en utilisant la chaîne de bits K_T et transmettre le secret crypté à Alice et Bob via les canaux classiques. Cependant, Alice et Bob doivent coopérer pour reconstruire le secret de Trent.

Avantages et inconvénients du protocole

- Aucune information classique n'est transmise pendant le protocole sauf pour le processus de détection, ce qui réduit le pourcentage d'espionnage ;
- Il empêche l'agent malhonnête ou le groupe d'agents non autorisés de tricher ;
- Toute écoute indiscrète provoquera des erreurs qui aideront à détecter l'intrusion ;
- La technologie de stockage quantique est requise pour la détection des écoutes clandestines ce qui peut être considéré comme un frein pour le protocole à cause de la difficulté de se procurer cette technologie ;
- Le protocole peut être généralisé pour le cas de N parties.

2.3 Synthèse

Jusqu'à aujourd'hui, de nombreux et divers protocoles de partage de secret quantique ont été proposés afin de permettre le partage de secret entre différentes personnes tout en maintenant la sécurité de la transmission.

Dans cette section, nous présentons une synthèse des six protocoles précédemment analysés. Ces derniers peuvent être regroupés en deux (02) catégories en fonction du nombre de participants dans chaque protocole. La première catégorie comprend les protocoles qui ont une limite en nombre de participants. Tandis que la deuxième catégorie comprend les protocoles qui n'ont aucune limite quant au nombre de participants.

Dans la première catégorie, nous retrouvons le premier protocole qui a été proposé par Deng et al. [15] dans le but de permettre à deux participants d'acquérir une clé secrète partagée, qu'ils utiliseront lorsqu'ils auront à travailler ensemble, et cela avec l'aide d'un tiers (l'expéditeur).

Pour modéliser le protocole, les idées de codage dense et du réarrangement de l'ordre des paires EPR ont été utilisées telle que l'idée de base du réarrangement d'ordre est que l'expéditeur mélange la corrélation correcte des particules dans les paires EPR de sorte qu'un espion ne sache pas quelles sont les deux particules dans une paire EPR et qu'il ne puisse pas effectuer de mesure de Bell pour voler les informations secrètes. Plus tard, l'expéditeur restaure la correspondance correcte des particules et obtient le résultat avec une mesure basée sur Bell.

Le second protocole étudié est proposé par Zhu et al. [27], il garantit un partage de secret sur de longues distances et ne souffre pas du problème d'atténuation d'intrication, qui provoque la rupture de l'intrication de deux particules dans le cas des longues distances. Pour la conception du protocole, des paires EPR et la porte contrôlée NOT (CNOT) ont été utilisées.

Enfin, nous avons analysé le protocole de téléportation bidirectionnel asymétrique contrôlé proposé par Choudhury et al [12] dans le but de permettre l'échange mutuel d'états quantiques de deux personnes, Alice (un état W généralisé à trois qubits) et Bob (un état intriqué arbitraire à deux qubits), en utilisant un état de cluster de 10 qubits comme canal de partage et cela sous la supervision d'une tierce partie Charlie.

Dans la deuxième catégorie, nous retrouvons le protocole proposé par Sun et al. [24] qui a pour but de permettre à des agents d'acquérir des clés partagées, qui seront utilisées pour concevoir la clé commune leur permettant de décrypter les messages secrets transmis par l'expéditeur. Les agents doivent ainsi coopérer. Pour modéliser le protocole, quatre états de Bell et deux états GHZ ont été utilisés.

Le second protocole étudié est proposé par Wang et al. [26] afin de permettre à un détenteur d'un secret quantique de le partager avec d'autres agents du réseau.

Pour cela, la transmission se fait couche par couche allant de la couche racine (le détenteur) vers la dernière couche où les agents qui la définissent coopérent ensemble pour pouvoir récupérer le secret.

Pour concevoir le protocole, les états GHZ et les mesures généralisées de la base Bell ont été utilisés. Ce protocole peut être utilisé dans les réseaux sans fil pour garantir la sécurité de la commmunication.

Enfin, dans le protocole proposé par Musanna et Kumar [20], des participants doivent s'entendre pour reconstruire le secret original transmis par un expéditeur. Pour élaborer le protocole, des états de Bell et les opérateurs de Pauli ont été utilisés. Le protocole proposé garantit un partage visuel secret parfait.

Une analyse des articles de la première catégorie montre que malgré les avantages offerts par les deux protocoles proposés par Deng et al. [15] et Zhu et al. [27], tous les deux sont confrontés au problème de la manipulation par l'adversaire qui pourrait affecter la sécurité de la transmission comparé au protocole proposé par Choudhury et al. [12], qui lui assure une protection contre ce type de problème.

En revanche, nous notons que contrairement à ces deux protocoles, les erreurs de mesure de l'un des participants dans le protocole proposé par Choudhury et al. [12] affectent les mesures des autres participants.

L'analyse des articles de la deuxième catégorie, nous permet de constater que les deux protocoles proposés par Sun et al. [24] et Wang et al. [26] assurent une protection contre le problème de la manipulation de l'adversaire à l'opposé du protocole proposé par Musanna et Kumar [20], qui lui est affecté par ce type de problème.

En revanche, d'après l'analyse faite sur les protocoles des deux catégories, nous constatons que bien que le protocole proposé par Musanna et Kumar [20] ne soit pas affecté par des erreurs de mesure, il fait face à des problèmes lors du partage de secret sur une longue distance, à l'inverse des protocoles proposés par Zhu et al. [27], Choudhury et al. [12] et Wang et al. [26], qui eux garantissent un partage optimal de secrets sur de longues distances.

Finalement, nous pouvons conclure que chaque protocole proposé comprend des avantages qui renforcent son efficacité, mais aussi des limites qui se dressent comme un obstacle, le plus répandu étant celui de la difficulté de la préparation des états intriqués.

Nombre de participants	Limité			Non Limité		
Critère \ Protocole	Deng et al. [15]	Zhu et al. [27]	Choudhury et al. [12]	Sun et al. [24]	Wang et al. [26]	Musanna et Kumar [20]
Utilisation d'états intriqués	✓	✓	✓	✓	✓	✓
États utilisés	Bell	Bell	W et Bell	GHZ et Bell	GHZ et Bell	Bell
Manipulation de l'adversaire	Oui	Oui	Non	Non	Non	Oui
Effet de la mesure sur les autres	Non	Non	Oui	N/A	N/A	Non
Partage sur longue distance	N/A	✓	✓	N/A	✓	✗

TABLE 2.1 – Comparaison des protocoles analysés.

2.4 Conclusion

Ce chapitre nous a permis de présenter un état de l'art sur les protocoles de partage quantique de secret. L'étude faite nous a permis d'une part de comprendre le fonctionnement de chaque protocole analysé, et d'autre part, de connaître les points forts de chaque protocole ainsi que leurs limites. Elle nous a également permis d'observer tous les points communs des protocoles ainsi que les différences entre eux.

Chapitre 3

Proposition et validation

3.1 Introduction

Le protocole proposé sera présenté dans ce chapitre. Tout d'abord, nous donnerons une description du protocole. Ensuite, nous fournirons un exemple illustratif du déroulement du protocole. Enfin, pour valider le protocole, nous considérerons sa sécurité.

3.2 Description du protocole

Nous proposons un protocole de partage de secret quantique déterministe, qui vise à permettre au propriétaire du secret de le partager avec d'autres parties participantes au protocole tout en garantissant la sécurité du partage contre tout intrus et la reconstruction du secret par les parties impliquées à la fin du protocole.

Le protocole proposé est un protocole impliquant quatre (04) parties, à savoir Alice qui tient le rôle du détenteur du secret et trois participants Bob1, Bob2 et Bob3, qui représentent les utilisateurs avec lesquels Alice souhaite partager le secret. Pour assurer un partage sécurisé du secret, les parties participant au protocole doivent suivre trois grandes phases que nous décrivons dans ce qui suit.

3.2.1 Phase d'envoi

C'est lors de cette phase que se fait l'envoi du secret par Alice aux trois utilisateurs. On suppose que Alice partage une clé secrète avec chacun des trois utilisateurs Bob1, Bob2 et Bob3, soient K_1, K_2 et K_3, respectivement. Les clés secrètes partagées seront utilisées dans notre protocole.

3.2.1.1 Étape 1

Alice génère des trios de particules dans l'un des états maximalement intriqués indiqués dans la Table 3.1.

La suite de trios de particules représente le secret que Alice souhaite partager avec les trois utilisateurs. Par exemple, si Alice souhaite partager la suite binaire 101, elle devra générer

trois particules quantiques dans l'état $|\psi_6\rangle$. Alice génère, en plus et aléatoirement, une suite de particules individuelles S_r dans l'un des états suivants $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

État intriqué	Représentation classique
$\|\psi_1\rangle = \frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$	000
$\|\psi_2\rangle = \frac{1}{\sqrt{2}}(\|000\rangle - \|111\rangle)$	111
$\|\psi_3\rangle = \frac{1}{\sqrt{2}}(\|001\rangle + \|110\rangle)$	001
$\|\psi_4\rangle = \frac{1}{\sqrt{2}}(\|001\rangle - \|110\rangle)$	110
$\|\psi_5\rangle = \frac{1}{\sqrt{2}}(\|010\rangle + \|101\rangle)$	010
$\|\psi_6\rangle = \frac{1}{\sqrt{2}}(\|010\rangle - \|101\rangle)$	101
$\|\psi_7\rangle = \frac{1}{\sqrt{2}}(\|011\rangle + \|100\rangle)$	011
$\|\psi_8\rangle = \frac{1}{\sqrt{2}}(\|011\rangle - \|100\rangle)$	100

TABLE 3.1 – États intriqués et leurs représentations classiques.

3.2.1.2 Étape 2

Alice envoie la suite de particules aux trois utilisateurs de la manière suivante : elle envoie la première particule de chaque trio dans l'état $|\psi_i\rangle$ et d'autres particules prises au hasard de S_r à Bob1. Elle en fait de même avec la deuxième et troisième particule de $|\psi_i\rangle$ qu'elle envoie respectivement à Bob2 et Bob3 accompagnées de particules prises aléatoirement de S_r. Il est à noter que l'emplacement des particules de S_r dépend des clés secrètes pré-partagées K_i. Ainsi, il sera difficile pour un intrus de distinguer entre les particules de S_r et celles portant l'information secrète.

3.2.1.3 Étape 3

Après avoir reçu la suite de particules envoyées par Alice, chacun des utilisateurs effectue l'une des trois transformations suivantes I, Z ou X sur la suite de toutes les particules reçues, avant de les renvoyer à Alice.

3.2.1.4 Étape 4

Après avoir reçu les particules transformées, Alice utilise les clés pré-partagées avec les utilisateurs pour reformer les trios initiaux de particules puis les mesure. Elle envoie ensuite les résultats de mesure aux trois utilisateurs. Une fois que les utilisateurs auront reçu les résultats par Alice, chacun utilisera sa clé secrète partagée avec Alice pour trouver l'emplacement exacte des particules issues du trio dans $|\psi_i\rangle$. Par exemple, les bits à 1 dans la clé secrète partagée dicteront l'emplacement des particules attribuées par Alice dans la suite envoyée, tandis que les bits à 0 dicteront l'emplacement des particules de S_r. La phase d'envoi ainsi clôturée, les utilisateurs peuvent passer à la phase de reconstruction du secret.

3.2.2 Phase de reconstruction du secret

Lors de cette phase, les trois parties doivent collaborer pour reconstruire le secret. En effet, il est difficile pour un seul utilisateur de deviner quelles transformations les deux autres utilisateurs ont pu effectuer sur les deux autres parties du trio de qubits intriqués. Ils doivent donc (1) s'échanger les transformations qu'ils ont choisies pour chaque trio, et (2) connaître l'état de ce trio après ces transformations (résultats de mesure que Alice a envoyés à la fin de la première phase), pour pouvoir remonter à l'état initial de chaque trio contenant le secret. Ils peuvent pour cela se référer aux tables présentées dans l'annexe A contenant tous les résultats des transformations possibles sur tous les états à trois qubits que Alice pourrait générer.

3.2.3 Phase de vérification du secret

Cette dernière phase a pour but de vérifier l'intégrité et la confidentialité de l'information quantique échangée durant le processus de partage du secret. Pour cela, Alice choisit au hasard des trios de particules, divulgue publiquement leur état initial et demande aux trois utilisateurs de divulguer publiquement ce qu'ils ont trouvé comme résultat. Si les deux états ne sont pas les mêmes, cela signifie qu'un intrus ou qu'au moins l'un des utilisateurs a essayé de lire l'information à partir d'une partie du trio et, par conséquent, a fait perdre le caractère d'intrication aux particules.

3.3 Exemple de déroulement du protocole

Dans cet exemple de déroulement, quatre (04) parties participent au protocole, à savoir Alice détenteur du secret et trois (03) utilisateurs Bob1, Bob2 et Bob3 avec lesquels Alice souhaite partager son secret.

3.3.1 Première phase

Cette première phase est la phase d'envoi durant laquelle Alice envoie son secret aux trois utilisateurs. Avant d'entamer les étapes de cette phase, Alice partage une clé secrète avec chacun des trois utilisateurs Bob1, Bob2 et Bob3 telles que

- $K_1 = 01001$, la clé secrète partagée entre Alice et Bob1 ;
- $K_2 = 10010$, la clé secrète partagée entre Alice et Bob2 ;
- $K_3 = 01010$, la clé secrète partagée entre Alice et Bob3.

3.3.1.1 Étape 1

Dans cet exemple, on suppose qu'Alice souhaite partager la suite binaire suivante : $\boxed{001010}$. Pour cela, elle devra commencer par générer trois (03) particules quantiques dans l'état $|\psi_3\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)$ pour pouvoir représenter la première partie de la suite binaire

qui est 001. Ensuite, elle devra générer trois (03) autres particules quantiques dans l'état $|\psi_5\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$ pour représenter la deuxième partie de la suite binaire qui est 010. Alice génère, en plus et aléatoirement, une suite de particules individuelles S_r dans l'un des états suivants $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

3.3.1.2 Étape 2

Alice envoie la suite de particules aux trois (03) utilisateurs. En prenant en compte les états intriqués et les clés pré-partagées, la suite des particules envoyées pour chaque utilisateur est la suivante :

- Pour Bob1, Alice envoie la suite de particules S_1 suivante :

  $S_1 = |1\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}, |+\rangle, |1\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}$.

- Pour Bob2, elle envoie la suite S_2 suivante :

  $S_2 = \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}, |-\rangle, |0\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}, |+\rangle$.

- Pour Bob3, elle envoie la suite S_3 suivante :

  $S_3 = |1\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}, |+\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}, |1\rangle$.

3.3.1.3 Étape 3

Après avoir reçu la suite de particules envoyées par Alice, chacun des utilisateurs effectue l'une des trois transformations sur la suite de toutes les particules reçues avant de les renvoyer à Alice. On suppose que les transformations effectuées sont les suivantes :

— $T_1 = \boxed{I, Z, X, I, Z}$ par Bob1 ;
— $T_2 = \boxed{Z, Z, X, X, I}$ par Bob2 ;
— $T_3 = \boxed{X, I, Z, I, I}$ par Bob3.

De ce fait, l'état des qubits sera transformé comme suit :

— Par Bob1 : $RT_1 = |0\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}, |-\rangle, |0\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)}$.

— Par Bob2 : $RT_2 = \boxed{\frac{1}{2}(|0\rangle\langle 0| - |1\rangle\langle 1|)}, -|-\rangle, |1\rangle, \boxed{\frac{1}{2}(|1\rangle\langle 0| + |0\rangle\langle 1|)}, |+\rangle$.

— Par Bob3 : $RT_3 = |0\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| - |1\rangle\langle 1|)}, |+\rangle, \boxed{\frac{1}{2}(|0\rangle\langle 0| - |1\rangle\langle 1|)}, |1\rangle$.

Après avoir transformé les particules, les trois (03) utilisateurs les envoient à Alice.

3.3.1.4 Étape 4

À la réception des particules, Alice rassemble les trios en se referant aux clés partagées et les mesure.

— Pour le premier trio, Alice aura comme résultat l'état $|\psi_3\rangle$ puisque $ZZI\,|\psi_3\rangle = |\psi_3\rangle$.
— Pour le second trio, Alice aura comme résultat l'état $|\psi_2\rangle$ puisque $ZXI\,|\psi_5\rangle = |\psi_2\rangle$.

Enfin, Alice annonce les résultats de mesure aux trois utilisateurs.

3.3.2 Deuxième phase

Pour la reconstruction du secret, deux informations sont requises, à savoir :

1. Les transformations faites sur chaque trio. En s'appuyant sur sa clé partagée avec Alice, chaque utilisateur sait quelle transformation il a faite sur chaque qubit du trio de qubits. Néanmoins, il a besoin de collaborer avec les autres utilisateurs pour connaître quelle transformation a pu subir tous le système à 3 qubits ;
2. L'état du résultat envoyé par Alice.

Pour cet exemple, la reconstruction du secret se fera en deux fois, étant donné que le secret est représenté par deux états. Dans un premier temps, les utilisateurs collaborent pour trouver l'état initial du premier trio envoyé par Alice. Pour cela, ils utilisent (1) le résultat de mesure $|\psi_3\rangle$ annoncé par Alice et (2) toutes les transformations faites sur ce trio qu'ils se sont échangées entre eux, dans ce cas

— Bob1 : Z.
— Bob2 : Z.
— Bob3 : Id.

Après avoir pris connaissance de ces deux informations, ils pourront les utiliser pour remonter à l'état initial envoyé par Alice, en s'aidant de la Table 3.2 qui regroupe toutes les transformations possibles sur tous les états possibles et qui donnent comme résultat final un système à 3 qubits dans l'état $|\psi_3\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	X	$\|\psi_3\rangle$
	Z	Z	X	
	X	X	Id	
$\|\psi_2\rangle$	Id	Z	X	$\|\psi_3\rangle$
	Z	Id	X	
	X	X	Z	
$\|\psi_3\rangle$	Id	Id	Id	$\|\psi_3\rangle$
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_4\rangle$	Id	Id	Z	$\|\psi_3\rangle$
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_5\rangle$	Id	X	X	$\|\psi_3\rangle$
	X	Id	Id	
	X	Z	Z	
$\|\psi_6\rangle$	Z	X	X	$\|\psi_3\rangle$
	X	Id	Z	
	X	Z	Id	
$\|\psi_7\rangle$	Id	X	Id	$\|\psi_3\rangle$
	Z	X	Z	
	X	Id	X	
$\|\psi_8\rangle$	Id	X	Z	$\|\psi_3\rangle$
	Z	X	Id	
	X	Z	X	

TABLE 3.2 – Tableau des états initiaux possibles pour l'état résultat $|\psi_3\rangle$.

En s'aidant de cette table et des informations requises obtenues, ils pourront déduire que l'état initial du trio était $|\psi_3\rangle$, et par conséquent, que la première partie du secret partagé est 001.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_3\rangle$	Z	Z	Id	$\|\psi_3\rangle$

TABLE 3.3 – État initial résultant des transformations faites par Bob1, Bob2 et Bob3 sur l'état $|\psi_3\rangle$.

Pour retrouver la deuxième partie du secret, ils devront collaborer de la même manière en s'aidant du résultat de mesure de Alice $|\psi_2\rangle$ et de la table 3.5 regroupant toutes les transformations possibles qui donneront un système dans l'état $|\psi_2\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	Z	$\|\psi_2\rangle$
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_2\rangle$	Id	Id	Id	$\|\psi_2\rangle$
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_3\rangle$	Id	Z	X	$\|\psi_2\rangle$
	Z	Id	X	
	X	X	Z	
$\|\psi_4\rangle$	Id	Id	X	$\|\psi_2\rangle$
	Z	Z	X	
	X	X	Id	
$\|\psi_5\rangle$	Id	X	Z	$\|\psi_2\rangle$
	Z	X	Id	
	X	Z	X	
$\|\psi_6\rangle$	Id	X	Id	$\|\psi_2\rangle$
	Z	X	Z	
	X	Id	X	
$\|\psi_7\rangle$	Z	X	X	$\|\psi_2\rangle$
	X	Id	Z	
	X	Z	Id	
$\|\psi_8\rangle$	Id	X	X	$\|\psi_2\rangle$
	X	Id	Id	
	X	Z	Z	

TABLE 3.4 – Tableau des états initiaux possibles pour un état résultat $|\psi_2\rangle$.

Les transformations faites sur ces qubits étant IXZ, les 3 utilisateurs déduiront que le système était initialement dans l'état $|\psi_5\rangle$ et que la deuxième partie du secret partagé est la suite 010.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_5\rangle$	Z	X	I	$\|\psi_2\rangle$

TABLE 3.5 – État initial résultant des transformations faites par Bob1, Bob2 et Bob3 sur l'état $|\psi_5\rangle$.

3.3.3 Tentatives illicites d'appropriation du secret partagé

Nous exposons dans ce qui suit les issues des tentatives d'appropriation du secret dans le cas de l'exemple de déroulement présenté précédemment. Les tableaux des états initiaux possibles pour tous les états finaux possibles sont répertoriés dans l'annexe A.

3.3.3.1 Cas de tentative interne

Dans le cas d'une tentative interne (i.e., d'un utilisateur participant au protocole), nous distinguons deux cas possibles décrits dans ce qui suit.

Cas de tentative d'un seul utilisateur

Dans le cas où l'un des trois utilisateurs voudrait s'approprier le secret en ne connaissant que la transformation qu'il a effectuée et l'état résultat envoyé par Alice, les résultats des tentatives pour chacun d'entre eux sont les suivants.

Bob1 : Il devra deviner entre sept (07) états qui sont représentés dans les Tables 3.6 et 3.7.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	Z	$\|\psi_2\rangle$
	Id	Z	Id	
$\|\psi_2\rangle$	Id	Id	Id	$\|\psi_2\rangle$
	Id	Z	Z	
$\|\psi_3\rangle$	Id	Z	X	$\|\psi_2\rangle$
$\|\psi_4\rangle$	Id	Id	X	$\|\psi_2\rangle$
$\|\psi_5\rangle$	Id	X	Z	$\|\psi_2\rangle$
$\|\psi_6\rangle$	Id	X	Id	$\|\psi_2\rangle$
$\|\psi_8\rangle$	Id	X	X	$\|\psi_2\rangle$

TABLE 3.6 – Tableau des états initiaux possibles pour l'état résultat $|\psi_2\rangle$ avec le choix Id pour T1.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	X	$\|\psi_3\rangle$
$\|\psi_2\rangle$	Id	Z	X	$\|\psi_3\rangle$
$\|\psi_3\rangle$	Id	Id	Id	$\|\psi_3\rangle$
	Id	Z	Z	
$\|\psi_4\rangle$	Id	Id	Z	$\|\psi_3\rangle$
	Id	Z	Id	
$\|\psi_5\rangle$	Id	X	X	$\|\psi_3\rangle$
$\|\psi_7\rangle$	Id	X	Id	$\|\psi_3\rangle$
$\|\psi_8\rangle$	Id	X	Z	$\|\psi_3\rangle$

TABLE 3.7 – Tableau des états initiaux possibles pour l'état résultat $|\psi_3\rangle$ avec le choix Id pour T1.

Bob2 : Il tombera sur sept (07) états pour chacun des états initiaux envoyés par Alice, et qui sont représentés dans les Tables 3.8 et 3.9.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_2\rangle$	X	X	X	$\|\psi_2\rangle$
$\|\psi_3\rangle$	X	X	Z	$\|\psi_2\rangle$
$\|\psi_4\rangle$	X	X	Id	$\|\psi_2\rangle$
$\|\psi_5\rangle$	Id	X	Z	$\|\psi_2\rangle$
	Z	X	Id	
$\|\psi_6\rangle$	Id	X	Id	$\|\psi_2\rangle$
	Z	X	Z	
$\|\psi_7\rangle$	Z	X	X	$\|\psi_2\rangle$
$\|\psi_8\rangle$	Id	X	X	$\|\psi_2\rangle$

TABLE 3.8 – Tableau des états initiaux possibles pour l'état résultat $|\psi_2\rangle$ avec le choix X pour T2.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Z	Z	X	$\|\psi_3\rangle$
$\|\psi_2\rangle$	Id	Z	X	$\|\psi_3\rangle$
$\|\psi_3\rangle$	Id	Z	Z	$\|\psi_3\rangle$
	Z	Z	Id	
$\|\psi_4\rangle$	Id	Z	Id	$\|\psi_3\rangle$
	Z	Z	Z	
$\|\psi_5\rangle$	X	Z	Z	$\|\psi_3\rangle$
$\|\psi_6\rangle$	X	Z	Id	$\|\psi_3\rangle$
$\|\psi_8\rangle$	X	Z	X	$\|\psi_3\rangle$

TABLE 3.9 – Tableau des états initiaux possibles pour l'état résultat $|\psi_3\rangle$ avec le choix Z pour T2.

Bob3 : Il tombera sur sept (07) états pour chacun des états initiaux envoyés par Alice, et qui sont représentés dans les Tables 3.10 et 3.11.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	Z	$\|\psi_2\rangle$
	Z	Z	Z	
$\|\psi_2\rangle$	Z	Id	Z	$\|\psi_2\rangle$
	Id	Z	Z	
$\|\psi_3\rangle$	X	X	Z	$\|\psi_2\rangle$
$\|\psi_5\rangle$	Id	X	Z	$\|\psi_2\rangle$
$\|\psi_6\rangle$	Z	X	Z	$\|\psi_2\rangle$
$\|\psi_7\rangle$	X	Id	Z	$\|\psi_2\rangle$
$\|\psi_8\rangle$	X	Z	Z	$\|\psi_2\rangle$

TABLE 3.10 – Tableau des états initiaux possibles pour l'état résultat $|\psi_2\rangle$ avec le choix Z pour T3.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_2\rangle$	X	X	Z	$\|\psi_3\rangle$
$\|\psi_3\rangle$	Z	Id	Z	$\|\psi_3\rangle$
	Id	Z	Z	
$\|\psi_4\rangle$	Id	Id	Z	$\|\psi_3\rangle$
	Z	Z	Z	
$\|\psi_5\rangle$	X	Z	Z	$\|\psi_3\rangle$
$\|\psi_6\rangle$	X	Id	Z	$\|\psi_3\rangle$
$\|\psi_7\rangle$	Z	X	Z	$\|\psi_3\rangle$
$\|\psi_8\rangle$	Id	X	Z	$\|\psi_3\rangle$

TABLE 3.11 – Tableau des états initiaux possibles pour l'état résultat $|\psi_3\rangle$ avec le choix Z pour T3.

Nous pouvons conclure par les résultats obtenus qu'aucun utilisateur seul ne peut parvenir à s'approprier le secret.

Cas de tentative de deux utilisateurs

Dans le cas où deux (02) utilisateurs s'entraideraient pour s'approprier le secret tout en ignorant les transformations faites par le troisième utilisateur, les résultats des tentatives sont présentés dans ce qui suit.

Bob1 et Bob2 : Ils tomberont sur trois (03) états pour chacun des états initiaux envoyés par Alice, et qui sont représentés dans les Tables 3.12 et 3.13.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_5\rangle$	Id	X	Z	$\|\psi_2\rangle$
$\|\psi_6\rangle$	Id	X	Id	$\|\psi_2\rangle$
$\|\psi_8\rangle$	Id	X	X	$\|\psi_2\rangle$

TABLE 3.12 – Tableau des états initiaux possibles pour l'état résultat $|\psi_2\rangle$ avec le choix Id pour T1 et X pour T2.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_2\rangle$	Id	Z	X	$\|\psi_3\rangle$
$\|\psi_3\rangle$	Id	Z	Z	$\|\psi_3\rangle$
$\|\psi_4\rangle$	Id	Z	Id	$\|\psi_3\rangle$

TABLE 3.13 – Tableau des états initiaux possibles pour l'état résultat $|\psi_3\rangle$ avec le choix Id pour T1 et Z pour T2.

Bob1 et Bob3 : Ils tomberont sur trois (03) états pour chacun des états initiaux envoyés par Alice, et qui sont représentés dans les Tables 3.14 et 3.15.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	Z	$\|\psi_2\rangle$
$\|\psi_2\rangle$	Id	Z	Z	$\|\psi_2\rangle$
$\|\psi_5\rangle$	Id	X	Z	$\|\psi_2\rangle$

TABLE 3.14 – Tableau des états initiaux possibles pour l'état résultat $|\psi_2\rangle$ avec le choix Id pour T1 et Z pour T3.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_4\rangle$	Id	Id	Z	$\|\psi_3\rangle$
$\|\psi_3\rangle$	Id	Z	Z	$\|\psi_3\rangle$
$\|\psi_7\rangle$	Id	X	Z	$\|\psi_3\rangle$

TABLE 3.15 – Tableau des états initiaux possibles pour l'état résultat $|\psi_3\rangle$ avec le choix Id pour T1 et Z pour T3.

Bob2 et Bob3 Ils tomberont sur trois (03) états pour chacun des états initiaux envoyés par Alice, et qui sont représentés dans les Tables 3.16 et 3.17.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_3\rangle$	X	X	Z	$\|\psi_2\rangle$
$\|\psi_5\rangle$	Id	X	Z	$\|\psi_2\rangle$
$\|\psi_6\rangle$	Z	X	Z	$\|\psi_2\rangle$

TABLE 3.16 – Tableau des états initiaux possibles pour l'état résultat $|\psi_2\rangle$ avec le choix X pour T2 et Z pour T3.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_3\rangle$	Id	Z	Z	$\|\psi_3\rangle$
$\|\psi_4\rangle$	Z	Z	Z	$\|\psi_3\rangle$
$\|\psi_5\rangle$	X	Z	Z	$\|\psi_3\rangle$

TABLE 3.17 – Tableau des états initiaux possibles pour l'état résultat $|\psi_3\rangle$ avec le choix Z pour T2 et Z pour T3.

Nous pouvons conclure par les résultats obtenus que pour chaque collaboration entre deux utilisateurs l'issue sera une chance sur trois (1/3) pour qu'ils parveniennent à s'approprier le secret.

3.3.3.2 Cas de tentative externe

Dans le cas où l'intrus Eve souhaiterait s'approprier le secret en ne connaissant que l'état résultat envoyé par Alice, elle tombera sur les huit (08) états initiaux et, de ce fait, n'aura aucune information sur le secret et ne pourra se l'approprier (voir annexe A).

3.4 Conclusion

Dans ce dernier chapitre, nous avons présenté notre protocole proposé pour la contribution dans le domaine du partage de secret quantique, en détaillant les différentes phases qui le composent. Une analyse des résultats de certains des tests effectués sur un exemple illustratif de déroulement du protocole est également fournie pour prouver son exactitude et sa fiabilité.

Conclusion générale

Le travail présenté dans ce mémoire a eu pour objectif de proposer un tout nouveau protocole de partage de secret quantique. Pour y parvenir, nous avons dû passer par trois étapes importantes.

La première étape de notre travail a consisté en l'étude de toutes les notations et définitions appartenant aux domaines sur lesquels repose notre thème, à savoir l'informatique, la cryptographie et le partage quantique de secret que nous avons présenté dans le premier chapitre.

Afin de suivre l'évolution des travaux dans le domaine du partage de secret quantique, nous avons consacré le deuxième chapitre à un état de l'art où nous avons étudié quelques protocoles et fait la comparaison entre eux.

Lors de la dernière étape, nous avons fait la proposition d'un tout nouveau protocole et sa validation, et cela, ne s'est fait qu'après avoir acquis les notions nécessaires qui nous ont permis d'y parvenir. Nous avons commencé par la description du protocole proposé, puis nous avons donné un exemple de son déroulement afin de valider sa faisabilité. Tout ce qui a été fait à cette étape a été rassemblé dans un chapitre consacré à notre contribution dans le domaine du partage de secret.

Nos Perspectives futures sont de :

- Valider davantage le protocole proposé et ne pas se référer qu'à la validation faite grâce à l'exemple.
- Généraliser le protocole de partage de secret proposé à un nombre d'utilisateurs supérieur à 3.
- Appliquer le protocole proposé à des domaines d'intelligence artificielle où le partage d'informations détient un rôle primordial tels que le Machine Learning et le Deep Learning.

Bibliographie

[1] Bit : définition. URL : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203567-bit-definition/. Consulté le 14 Septembre 2021.

[2] Comment fonctionne un ordinateur quantique ? URL : https://www.inria.fr/fr/comment-fonctionne-un-ordinateur-quantique. Consulté le : 16 Septembre 2021.

[3] Informatique quantique. URL : https://fr.wikipedia.org/w/index.php?title=Informatique_quantique&oldid=183688499. Consulté le : 14 Septembre 2021.

[4] Introduction à la cryptographie. URL : http://www.cryptage.org/introduction.html. Consulté le 20 Septembre 2021.

[5] Le qubit en informatique quantique - Azure Quantum. URL : https://docs.microsoft.com/fr-fr/azure/quantum/concepts-the-qubit. Consulté le : 16 Septembre 2021.

[6] Porte quantique. URL : https://fr.wikipedia.org/w/index.php?title=Porte_quantique&oldid=184385486. Consulté le : 15 Septembre 2021.

[7] Que signifie Qubit ? - Definition IT de Whatis.fr. URL : https://www.lemagit.fr/definition/Qubit. Consulté le 14 Septembre 2021.

[8] Spellbook - Cryptologie - Terminologie. URL : http://cryptologie.free.fr/crypto/terminologie.html. Consulté le 20 Septembre 2021.

[9] Ordinateur quantique : 6. Introduction au fonctionnement de l'ordinateur quantique, November 2018. URL : https://www.gbnews.ch/ordinateur-quantique-6-introduction-au-fonctionnement-de-lordinateur-quantique/. Consulté le : 16 Septembre 2021.

[10] Thameur Abdelli. Ordinateur quantique : 5. Introduction au fonctionnement de l'ordinateur classique. 2018. URL : :https://www.gbnews.ch/ordinateur-quantique-5-introduction-au-fonctionnement-de-lordinateur-classique/.Consultéle:14Septembre2021.

[11] Gilles Van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, June 2006.

[12] Binayak S. Choudhury and Soumen Samanta. Asymmetric bidirectional quantum state exchange between alice and bob through a third party. *Optik*, 231 :166435, 2021.

[13] P Communauté and ORE. La Téléportation quantique : tout ce qu'il faut savoir, January 2020. URL : https://www.institut-pandore.com/physique-quantique/teleportation-quantique-intrication-quantique/. Consulté le : 16 Septembre 2021.

[14] Bastien Contreras. Informatique quantique : où en est-on ? URL : https://www.clubic.com/technologies-d-avenir/actualite-854536-informatique-quantique.html. Consulté le : 16 Septembre 2021.

[15] Fu-Guo Deng, Gui Lu Long, and Hong-Yu Zhou. An efficient quantum secret sharing scheme with einstein–podolsky–rosen pairs. *Physics Letters A*, 340(1) :43–50, 2005.

[16] Renaud Dumont. *Cryptographie et Sécurité informatique*, volume 2010. 2009.

[17] Jérome Javelle. *Cryptographie Quantique : Protocoles et Graphes*. PhD thesis. URL : https://tel.archives-ouvertes.fr/tel-01215912. Consulté le : 15 Septembre 2021.

[18] Jacques Lederer. QU'EST-CE QUE L'INFORMATIQUE ? (Informaticinfo). URL : https://www.informaticinfo.com/computer_science_def_frames_fr.html. Consulté le : 14 Septembre 2021.

[19] Pontoise Marjorie. Les DRM (Digital Rights Management). URL : https://www.memoireonline.com/02/07/355/m_les-drm-digital-rights-management7.html. Consulté le 06 Octobre 2021.

[20] Farhan Musanna and Sanjeev Kumar. A novel three-party quantum secret sharing scheme based on bell state sequential measurements with application in quantum image sharing. *Quantum Inf Process*, 19(348), 2020.

[21] El Mrabet Nadia. Les concepts fondamentaux de la cryptographie. URL : https://docplayer.fr/44708522-Les-concepts-fondamentaux-de-la-cryptographie.html. Consulté le : 20 Septembre 2021.

[22] Laurent Sacco. Ordinateur quantique. URL : https://www.futura-sciences.com/sciences/definitions/physique-ordinateur-quantique-4348/. Consulté le : 14 Septembre 2021.

[23] Delestan Serge and Lejeune Lionel. Chiffrement & cryptographie - Aspect technique. *Chiffrement & cryptographie*. URL : http://nopb.chez.com/crypto2.html. Consulté le 19 Septembre 2021.

[24] Ying Sun, Qiao yan Wen, Fei Gao, Xiu bo Chen, and Fu chen Zhu. Multiparty quantum secret sharing based on bell measurement. *Optics Communications*, 282(17) :3647–3651, 2009.

[25] Céline Thuillet. *Implantations cryptographiques sécurisées et outils d'aide à la validation des contremesures contre les attaques par canaux cachés*. Thèse de doctorat, Université de Bordeaux 1, 2012.

[26] Xiao-Jun Wang, Long-Xi An, Xu-Tao Yu, and Zai-Chen Zhang. Multilayer quantum secret sharing based on ghz state and generalized bell basis measurement in multiparty agents. *Physics Letters A*, 381(38) :3282–3288, 2017.

[27] ZC Zhu, Hu AQ, and Fu. Two new controlled not gate based quantum secret sharing protocols without entanglement attenuation. *Int J Theor Phys*, page 55, 2016.

Annexe A

Résultats des transformation possibles

Dans cette annexe, nous présentons sous forme de tables tous les états finaux des qubits qui peuvent résulter de toutes les tranformations possibles faites sur tous les états initiaux de ces qubits.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	Id	
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_2\rangle$	Id	Id	Z	
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_3\rangle$	Id	Id	X	
	Z	Z	X	
	X	X	Id	
$\|\psi_4\rangle$	Id	Z	X	
	Z	Id	X	$\|\psi_1\rangle$
	X	X	Z	
$\|\psi_5\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	
$\|\psi_6\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	
$\|\psi_7\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	
$\|\psi_8\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	

TABLE A.1 – États initiaux possibles pour l'état résultat $|\psi_1\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	Z	
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_2\rangle$	Id	Id	Id	
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_3\rangle$	Id	Z	X	
	Z	Id	X	
	X	X	Z	
$\|\psi_4\rangle$	Id	Id	X	
	Z	Z	X	$\|\psi_2\rangle$
	X	X	Id	
$\|\psi_5\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	
$\|\psi_6\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	
$\|\psi_7\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	
$\|\psi_8\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	

TABLE A.2 – États initiaux possibles pour l'état résultat $|\psi_2\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Id	X	
	Z	Z	X	
	X	X	Id	
$\|\psi_2\rangle$	Id	Z	X	
	Z	Id	X	
	X	X	Z	
$\|\psi_3\rangle$	Id	Id	Id	
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_4\rangle$	Id	Id	Z	
	Id	Z	Id	
	Z	Id	Id	$\|\psi_3\rangle$
	Z	Z	Z	
$\|\psi_5\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	
$\|\psi_6\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	
$\|\psi_7\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	
$\|\psi_8\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	

TABLE A.3 – États initiaux possibles pour l'état résultat $|\psi_3\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	Z	X	
	Z	Id	X	
	X	X	Z	
$\|\psi_2\rangle$	Id	Id	X	
	Z	Z	X	
	X	X	Id	
$\|\psi_3\rangle$	Id	Id	Z	
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_4\rangle$	Id	Id	Id	
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	$\|\psi_4\rangle$
	X	X	X	
$\|\psi_5\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	
$\|\psi_6\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	
$\|\psi_7\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	
$\|\psi_8\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	

TABLE A.4 – États initiaux possibles pour l'état résultat $|\psi_4\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	
$\|\psi_2\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	
$\|\psi_3\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	
$\|\psi_4\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	
$\|\psi_5\rangle$	Id	Id	Id	
	Id	Z	Z	$\|\psi_5\rangle$
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_6\rangle$	Id	Id	Z	
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_7\rangle$	Id	Id	X	
	Z	Z	X	
	X	X	Id	
$\|\psi_8\rangle$	Id	Z	X	
	Z	Id	X	
	X	X	Z	

TABLE A.5 – États initiaux possibles pour l'état résultat $|\psi_5\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	
$\|\psi_2\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	
$\|\psi_3\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	
$\|\psi_4\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	
$\|\psi_5\rangle$	Id	Id	Z	
	Id	Z	Id	$\|\psi_6\rangle$
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_6\rangle$	Id	Id	Id	
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_7\rangle$	Id	Z	X	
	Z	Id	X	
	X	X	Z	
$\|\psi_8\rangle$	Id	Id	X	
	Z	Z	X	
	X	X	Id	

TABLE A.6 – États initiaux possibles pour l'état résultat $|\psi_6\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	
$\|\psi_2\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	
$\|\psi_3\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	
$\|\psi_4\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	
$\|\psi_5\rangle$	Id	Id	X	
	Z	Z	X	$\|\psi_7\rangle$
	X	X	Id	
$\|\psi_6\rangle$	Id	Z	X	
	Z	Id	X	
	X	X	Z	
$\|\psi_7\rangle$	Id	Id	Id	
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	
$\|\psi_8\rangle$	Id	Id	Z	
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	

TABLE A.7 – États initiaux possibles pour l'état résultat $|\psi_7\rangle$.

Initial	Bob1	Bob2	Bob3	Résultat
$\|\psi_1\rangle$	Z	X	X	
	X	Id	Z	
	X	Z	Id	
$\|\psi_2\rangle$	Id	X	X	
	X	Id	Id	
	X	Z	Z	
$\|\psi_3\rangle$	Id	X	Z	
	Z	X	Id	
	X	Z	X	
$\|\psi_4\rangle$	Id	X	Id	
	Z	X	Z	
	X	Id	X	
$\|\psi_5\rangle$	Id	Z	X	
	Z	Id	X	$\|\psi_8\rangle$
	X	X	Z	
$\|\psi_6\rangle$	Id	Id	X	
	Z	Z	X	
	X	X	Id	
$\|\psi_7\rangle$	Id	Id	Z	
	Id	Z	Id	
	Z	Id	Id	
	Z	Z	Z	
$\|\psi_8\rangle$	Id	Id	Id	
	Id	Z	Z	
	Z	Id	Z	
	Z	Z	Id	
	X	X	X	

TABLE A.8 – États initiaux possibles pour l'état résultat $|\psi_8\rangle$.

Résumé

Afin de maintenir la confidentialité des informations partagées, plusieurs protocoles ont vu le jour au fil des temps. Avec l'évolution des humains, s'en suit l'évolution des moyens, des techniques et des protocoles qui ont été développés pour répondre à cette attente. C'est notamment grâce à la cryptographie que de tels protocoles ont pu être développés. Parmi les protocoles proposés pour le maintien de la sécurité du partage de secret, certains demeurent toujours d'actualité tandis que d'autres se sont retirés après avoir connu une époque de gloire. Dans ce mémoire, nous nous sommes concentrés sur les protocoles qui appartiennent à une branche importante de la cryptographie quantique qui est le partage de secret pour pouvoir à la fin proposer à notre tour un tout nouveau protocole de partage de secret quantique.

Mots clés : confidentialité, partage de secret quantique, cryptographie quantique.

Abstract

In order to maintain the confidentiality of shared information, several protocols have emerged over time. With the evolution of humans, follows the evolution of the means, techniques and protocols which have been developed to meet this expectation. It is in particular thanks to cryptography that such protocols have been developed. Among the protocols proposed for maintaining the security of secret sharing, some are still valid while others have withdrawn after a period of glory. In this thesis, we have focused on the protocols that belong to an important branch of quantum cryptography, which is secret sharing in order to be able to finally propose in our turn a whole new protocol for quantum secret sharing.

Keywords : confidentiality, quantum secret sharing, quantum cryptography.