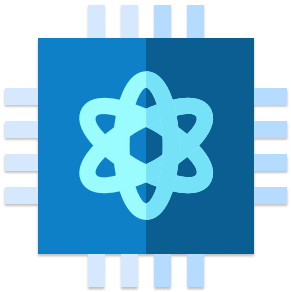


Cryptographie quantique

Rédigé au semestre de printemps 2020 par :

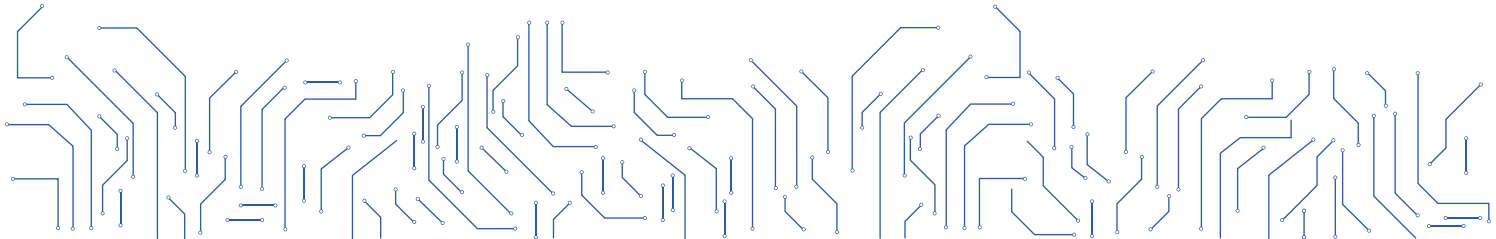
Alexandre DESBOS

Université :

Université de Technologie de Belfort-Montbéliard

Enseignant chercheur encadrant :

Frédéric Holweck



Avant-propos

Ce rapport est écrit dans le cadre de la validation de l'unité de valeur Acquisition de Connaissances et plus largement dans l'obtention du diplôme d'ingénieur en génie informatique à l'Université de Technologie de Belfort-Montbéliard.

Bien que le choix de l'unité de valeur m'ait d'abord été imposé, il s'est avéré que mon professeur encadrant, monsieur Frédéric HOLWECK, m'a proposé d'entrer et de découvrir un monde passionnant, celui de l'informatique quantique et plus particulièrement de la cryptographie quantique théorique. J'ai porté un intérêt à ce domaine par curiosité mais aussi parce que c'est un sujet actuel et qui va probablement prendre de l'ampleur dans les années à venir.

L'objectif de ce rapport est donc de faire ses premiers pas dans le monde de l'infiniment petit en explorant d'abord les principes fondamentaux de l'informatique quantique puis en cherchant à comprendre deux protocoles de cryptographie quantique, ces protocoles étant peut être de futures normes de communications dans le domaine des transmissions de données.

Les principales difficultés ont été liées aux différentes notations utilisées dans les documents sources d'informations sur le sujet. Certains de ces documents étaient à destination de personnes déjà averties et donc plutôt inaccessibles pour un novice.

Remerciements

Je souhaite remercier tout particulièrement mon professeur tuteur, monsieur Frédéric Holweck, qui a pris le temps de m'appeler, de m'expliquer et de me guider pendant mes recherches malgré la période très particulière pendant laquelle nous avons travaillé ensemble. Il m'a permis d'accéder au **monde quantique**, un univers très intéressant qui me paraissait être à des **années lumières** de mes compétences.

J'aimerais remercier l'UTBM, pour avoir accepté ma candidature et m'avoir permis d'être étudiant ingénieur.

Finalement, je voudrais remercier le directeur de cette école, monsieur Gishlain Montavon, ainsi que toute l'équipe pédagogique qui s'est mobilisée pendant cette période difficile afin de permettre à tous les étudiants de continuer à travailler dans les meilleures conditions. Certains voient cette période comme une difficulté, je la vois comme une expérience qui nous renforce toutes et tous.

Merci.

Table des matières

Chapitre 1

Introduction

Une quantité de données astronomique est produite et échangée à travers le monde. L'Internet contribue massivement à cette production titanesque de données.
Voici quelques chiffres bluffants :

- En 2018, **280 Milliards** d'e-mails étaient envoyés par jour.
- **75 Milliards** d'utilisateurs de Uber par mois, chaque véhicule étant géolocalisé en temps réel.
- **23 000 Milliards** de messages Whatsapp et **6000 Milliards** de SMS échangés par an.
- D'ici 2025, nous pourrions atteindre une quantité de données totale produite de 175 zetta bits [1], ce qui équivaut à : **175 000 000 000 000 000 000 000** bits de données.

Il existe des centaines d'exemples statistiques montrant la quantité démesurée de données que nous produisons. Dès lors, il vient la question de sécurité. C'est un point non négligeable auquel nous pensons en lisant ces chiffres. Comment transférer la localisation du véhicule Uber du smartphone du conducteur vers les serveurs de l'entreprise, sans qu'elle ne puisse être interceptée, interprétée et vendue au plus offrant ? Comment crypter les conversations entre deux personnes qui pourraient s'échanger des informations "délicates" ou comment crypter le transfert de données d'un routeur à un serveur lorsque l'on effectue une transaction bancaire sur un site web localisé à l'autre bout de la planète ?
Ce sont des questions auxquelles nous pouvons apporter des réponses grâce aux technologies d'aujourd'hui. Mais qu'en est-il des technologies de demain ? Les enjeux vis à vis des données ne cessent de grandir et la cryptographie quantique pourrait être une solution pour améliorer les protocoles de sécurité du présent et imaginer ceux du futur.
Dans ce rapport, nous aborderons d'abord les bases de l'informatique quantique qui nous permettront ensuite de présenter deux protocoles de cryptographie quantique.

1. Data Age 2025, Seagate - data from IDC global datasphere - November 2018

Chapitre 2

Principes fondamentaux de l'informatique quantique

2.1 Le bit quantique et les états quantiques

En informatique, le bit est la quantité minimale d'information d'un message, c'est l'unité de mesure de base. Il ne peut prendre que deux valeurs : 0 ou 1 qui peuvent représenter soit une alternative logique (vrai/faux) soit un chiffre du système binaire. En informatique quantique, il existe un analogue du bit appelé **qubit** (prononcé /kju.bit/) représentant un système quantique à 2 états. Ces deux états sont notés $|0\rangle$ et $|1\rangle$ (prononcé "ket 0" et "ket 1"), notation introduite par Paul Dirac [1] en 1939. Tandis que le bit ne peut prendre que deux valeurs, le qubit lui, peut se trouver dans une infinité d'états entre $|0\rangle$ et $|1\rangle$. L'état du qubit est noté $|\phi\rangle$ dans la base $(|0\rangle, |1\rangle)$.

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \alpha, \beta \in \mathbb{C} \tag{2.1}$$

Lorsque l'on mesure l'état du qubit dans la base $(|0\rangle, |1\rangle)$, le qubit est projeté sur un des états selon une certaine probabilité : $|\alpha|^2$ est la probabilité d'obtenir $|0\rangle$ et $|\beta|^2$ est la probabilité d'obtenir $|1\rangle$.
Ainsi, $|\alpha|^2 + |\beta|^2 = 1$.

2.2 Notation de Dirac Bra-Ket

Notation de Dirac [1] :

$$\langle u|v\rangle \tag{2.2}$$

Cette notation a d'abord été inventée comme alternative à la notation du produit scalaire $\langle , \rangle$. Ici, $|u\rangle$ est prononcé "**ket** de u" et $\langle v|$ est prononcé "**bra** de v".

1. Paul Adrien Maurice Dirac est un mathématicien et physicien britannique, un des pères de la mécanique quantique

En utilisant une notation matricielle pour représenter l'état d'un système, on a :

$$|\phi\rangle = \begin{pmatrix} a_1 \\ . \\ . \\ . \\ a_n \end{pmatrix} \qquad \langle\phi| = \begin{pmatrix} \overline{a_1} & ... & \overline{a_n} \end{pmatrix}$$

Effectuer le produit scalaire $\langle\phi|\phi\rangle$, revient donc à multiplier la matrice ligne par la matrice colonne ci-dessus :

$$\langle\phi|\phi\rangle = \begin{pmatrix} \overline{a_1} & ... & \overline{a_n} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ . \\ . \\ . \\ a_n \end{pmatrix} = \overline{a_1} \cdot a_1 + ... + \overline{a_n} \cdot a_n$$

2.3 Les postulats de l'informatique quantique simplifiés

Une expérience physique peut être divisée en 2 parties : la préparation et la mesure. La première partie va définir les résultats possibles de l'expérience, alors que la seconde partie a pour but de récupérer la valeur des résultats. Mais en physique quantique, la situation est un petit peu différente. Nous avons vu dans la partie 2.1 sur le qubit que celui ci avait une certaine probabilité d'être mesuré dans un état ou dans un autre. En effet, lors de la première partie (la préparation), le but est de définir les **probabilités** des différents résultats possibles de l'expérience contrairement à la physique "classique" ou les résultats sont **déterministes**[1]. La différence est notable sur la seconde partie aussi car les mesures donnent les résultats de manières statistiques. On répète les expériences un grand nombre de fois pour obtenir les résultats. Nous allons maintenant présenter les postulats de l'informatique quantique [15] nécessaires à la compréhension de ce rapport.

Axiome 1 : Le principe de superposition quantique

Un système quantique est représenté par un vecteur d'un espace vectoriel nommé espace de Hilbert (ou espace des états), noté $\mathcal{H}$.
Cet espace vectoriel est complexe et muni du produit scalaire hermitien.

Produit scalaire dans $\mathcal{H}$

Un produit scalaire hermitien est une application qui à deux vecteurs associe un nombre complexe, dans le cas de l'espace de Hilbert, c'est une application qui à un "bra" et à un "ket" fait correspondre un nombre complexe $z = \langle\psi|\phi\rangle$, vérifiant les propriétés suivantes :

- Positivité : $\langle\phi|\phi\rangle \geq 0$, l'égalité étant vraie seulement pour $|\phi\rangle = 0$
- Semi-linéarité par rapport à la première variable :
  Soit $\langle\psi_1|, \langle\psi_2| \in \mathcal{H}^*$, $|\phi\rangle \in \mathcal{H}$ et $z_1, z_2 \in \mathbb{C}$

$$\langle z_1\psi_1 + z_2\psi_2|\phi\rangle = \overline{z_1}\langle\psi_1|\phi\rangle + \overline{z_2}\langle\psi_2|\phi\rangle$$

1. Théorie selon laquelle la succession des évènements et des phénomènes est due au principe de cause à effet.

- Linéarité par rapport à la 2ème variable
  Soit $\langle\psi| \in \mathcal{H}^*$, $|\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}$ et $z_1, z_2 \in \mathbb{C}$
$$\langle\psi|z_1\phi_1 + z_2\phi_2\rangle = z_1 \langle\psi|\phi_1\rangle + z_2 \langle\psi|\phi_2\rangle$$
- $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^*$

Principe de superposition

Le vecteur $|\phi\rangle$ de l'espace de Hilbert peut être décomposé en une combinaison linéaire de vecteurs dans une base donnée. C'est ainsi qu'on a décrit le qubit dans l'équation (2.1), mais on peut faire de même pour n'importe quelle base de l'espace de Hilbert.

Soit $(|e_1\rangle, |e_2\rangle, ..., |e_n\rangle), n \in \mathbb{N}$, une base de $\mathcal{H}$, l'état $|\phi\rangle$ peut être écrit comme combinaison linéaire des états $|e_i\rangle, i \in [1; n]$:
$$|\phi\rangle = \sum_{i=1}^{n} a_i \cdot |e_i\rangle \tag{2.3}$$

Dans notre cas, nous travaillerons en dimensions finies et nous utiliserons les représentations matricielles des états des systèmes étudiés. Dans la base $(|0\rangle, |1\rangle)$, on peut donc noter :
$$|0\rangle \to \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle \to \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Axiome 2 : Les mesures

Mesure d'un qubit

Dans l'équation (2.3) :
$$|\phi\rangle = \sum_{i=1}^{n} a_i \cdot |e_i\rangle$$

Les amplitudes complexes a_i vérifient :
$$|a_1|^2 + ... + |a_n|^2 = 1$$
avec $|a_i|^2$ la probabilité d'observer $|e_i\rangle$ quand on mesure l'état de $|\phi\rangle$ dans la base $(|e_1\rangle, |e_2\rangle, ..., |e_n\rangle)$

Observables

Il est important de définir la notion d'**observable** lorsque l'on mesure en physique quantique :
pour toute propriété physique $\mathcal{A}$ (Spin, moment angulaire, énergie...), il existe un opérateur Hermitien linéaire associé noté A et A est un **observable** dans $\mathcal{H}$.
Autrement dit, soit A une matrice de $\mathcal{H}$, A est Hermitienne si A est égale à sa transposée conjuguée :
$$\forall |\phi\rangle, |\psi\rangle \in \mathcal{H}, \langle A\phi|\psi\rangle = \langle\phi|A\psi\rangle \iff A = {}^t A^*$$

Les valeurs propres de A sont les valeurs possibles de la propriété physique et les vecteurs propres correspondants sont les états dans lequel est projeté le système après la mesure.

Axiome 3 : État du qubit après la mesure

En physique quantique, lorsqu'un système est en superposition de plusieurs états et qu'on le mesure, ce système est réduit à **un seul** état. C'est ce qu'on appelle la réduction du paquet d'onde.
Ainsi, lorsque l'état d'un qubit est mesuré dans la base $(|e_1\rangle, |e_2\rangle, ..., |e_n\rangle)$, l'état $|\phi\rangle$ est projeté sur un des états de bases $|e_i\rangle$.

Axiome 4 : Évolution dans le temps de l'état du qubit

L'évolution d'un système fermé (qui n'a aucune interaction avec un système extérieur) est unitaire. L'état $|\phi(t)\rangle$ à l'instant t dépend de l'état $|\phi(t_0)\rangle$ à l'instant t_0 en appliquant un opérateur unitaire $U(t, t_0)$:

$$|\phi(t)\rangle = U(t, t_0)\,|\phi(t_0)\rangle$$

Remarque : On dit d'une matrice U carrée d'ordre n et à coefficients complexes qu'elle est **unitaire** si elle vérifie : $U \cdot U^\dagger = U^\dagger \cdot U = I_n$
Remarque : Le symbole †, se prononce "dagger" (= dague) et signifie "transposée conjuguée".

La machine quantique d'IBM

Dans le reste du rapport, nous utiliserons la machine quantique d'IBM : IBM Quantum experience [17]. Cette machine est mise à disposition du grand public et nous permettra de manipuler des qubits. L'interface graphique de l'outil d'IBM nous permet de créer graphiquement des circuits quantiques. Les qubits sont représentés par un fil et sont initialement dans l'état $|0\rangle$. On peut alors manipuler l'état des qubits en leur appliquant des matrices unitaires (représentées par des portes quantiques, que nous aborderons dans la partie 2.5). Finalement, on peut mesurer l'état de ces qubits en appliquant l'opérateur de mesure.

Exemple

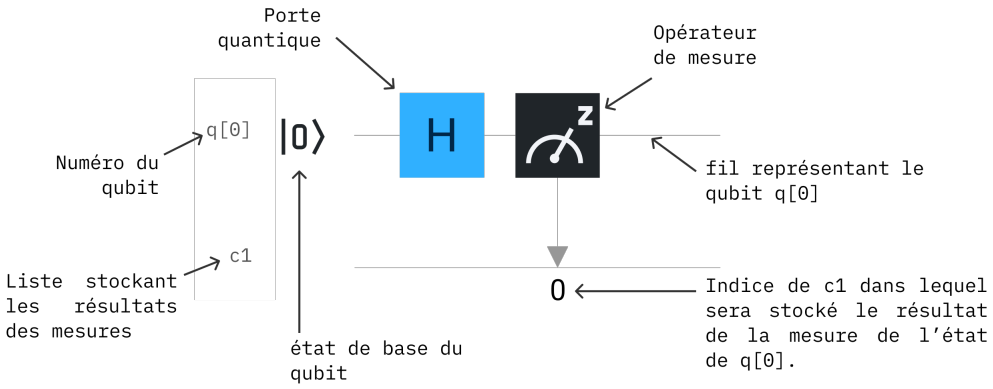


FIGURE 2.1 – Exmple de circuit sur IBM QX

Dans cet exemple, nous appliquons la matrice unitaire $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, représentée par la porte quantique H, à l'état du qubit q[0].
Ensuite, on applique la porte mesure afin de mesurer l'état du qubit q[0], puis le résultat est conservé dans la liste $c1$ à l'indice 0.

Ici le résultat sera théoriquement :

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

Autrement dit, d'après l'axiome 2 de la partie 2.3, on a statistiquement 50% de chance de mesurer $|0\rangle$ et 50% de chance de mesurer $|1\rangle$.

2.4 La sphère de Bloch

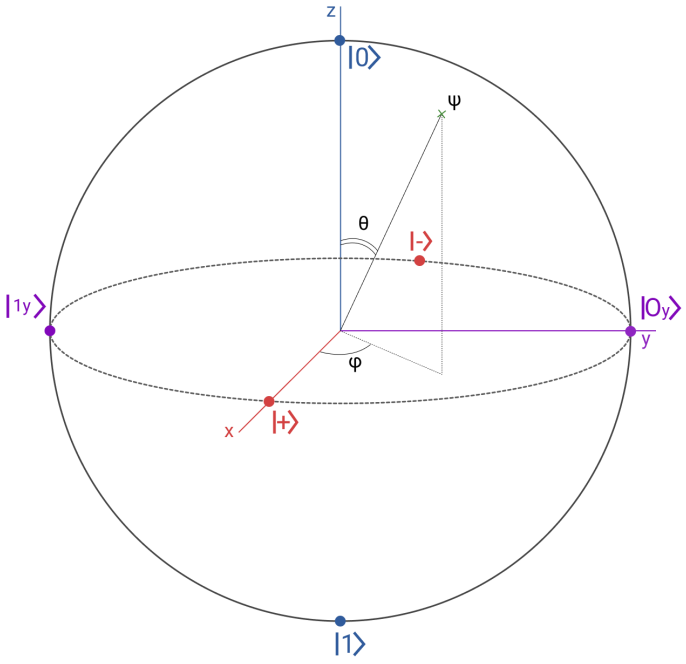


FIGURE 2.2 – Sphère de Bloch

La sphère de Bloch [5] est une représentation géométrique d'un système quantique à deux états, ce qui est parfait pour représenter un qubit de la forme : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

On peut noter que l'état de ce qubit peut être exprimé, à une phase globale près, en coordonnées sphériques par :

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) \cdot |0\rangle + e^{i\phi} \cdot \sin\left(\frac{\theta}{2}\right) |1\rangle$$

$$\text{avec } \theta \in [0;\pi], \phi \in [0;2\pi[\text{ et } e^{i\phi} = \cos(\phi) + i \cdot \sin(\phi)$$

Les pôles nord et sud de la sphère représentent les états de base $|0\rangle$ et $|1\rangle$.

Écrivons les états $|+\rangle, |-\rangle, |1_y\rangle$ et $|0_y\rangle$ en fonction de la base $(|0\rangle, |1\rangle)$:

$$|+\rangle = cos(\frac{\frac{\pi}{2}}{2}) |0\rangle + e^{i0} \cdot sin(\frac{\frac{\pi}{2}}{2}) |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = cos(\frac{\frac{-\pi}{2}}{2}) |0\rangle + e^{i0} \cdot sin(\frac{\frac{-\pi}{2}}{2}) |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|0_y\rangle = cos(\frac{\frac{-\pi}{2}}{2}) |0\rangle + e^{-i\pi/2} sin(\frac{\frac{\pi}{2}}{2}) |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$$

$$|1_y\rangle = cos(\frac{\frac{-\pi}{2}}{2}) |0\rangle + e^{i\pi/2} sin(\frac{\frac{\pi}{2}}{2}) |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$$

La base $(|+\rangle, |-\rangle)$ est appelée base Hadamard.

2.4.1 Protocole de mesure de l'état d'un qubit dans une base quelconque à l'aide de l'ordinateur quantique d'IBM

On sait que l'état $|\psi\rangle$ d'un qubit, représenté par un point de coordonnées (x, y, z) sur la sphère de Bloch peut être décrit à l'aide de coordonnées sphériques :

$$\begin{cases} x &= sin(\theta)cos(\phi) \\ y &= sin(\theta)sin(\phi) \\ z &= cos(\theta) \end{cases}$$

Ainsi, dans le cas de la machine d'IBM qui ne mesure **que** dans la base Z, pour mesurer dans une base quelconque B, il est nécessaire de :

- Calculer la matrice de passage P de la base Z vers la base B.
- Calculer la matrice conjuguée transposée de P, notée $P^\dagger$
- Mesurer $P^\dagger |\psi\rangle$ dans la base Z

Première étape :

La mesure d'un observable de la forme : $\mathcal{O} = \alpha X + \beta Y + \gamma Z$ est une tâche relativement aisée car les coefficient α, β et γ peuvent être exprimés :

$$\begin{cases} \alpha & = sin(\theta)cos(\phi) \\ \beta & = sin(\theta)sin(\phi) \\ \gamma & = cos(\theta) \end{cases}$$

Résoudre ce système nous permet ainsi de trouver θ et ϕ. Ces angles nous permettront ensuite de paramétrer la porte U3 qui sera appliquée avant la mesure de l'état d'un qubit sur la machine d'IBM.

Soit, U_3 une porte quantique qui donne une instruction à l'ordinateur quantique (nous parlerons des portes quantiques plus en détail dans le chapitre suivant 2.5) :

$$U_3(\theta, \phi, \lambda) = \begin{pmatrix} cos(\frac{\theta}{2}) & -e^{i\lambda}sin(\frac{\theta}{2}) \\ e^{i\phi}sin(\frac{\theta}{2}) & e^{i(\phi+\lambda)}cos(\frac{\theta}{2}) \end{pmatrix}$$

On peut déterminer la matrice de passage P à l'aide de θ et ϕ :

$$P = U_3(\theta, \phi, \lambda = 0) = \begin{pmatrix} cos(\frac{\theta}{2}) & -sin(\frac{\theta}{2}) \\ e^{i\phi}sin(\frac{\theta}{2}) & e^{i\phi}cos(\frac{\theta}{2}) \end{pmatrix}$$

Deuxième étape :

Il nous faut maintenant trouver la matrice conjuguée transposée de P, ainsi que trouver les paramètres $(\theta', \phi', \lambda')$ qui nous permettront de régler la porte U_3 que nous utiliserons avant la mesure. :

$$P^\dagger = ^\intercal (\overline{P}) = \begin{pmatrix} cos(\frac{\theta}{2}) & e^{-i\phi}sin(\frac{\theta}{2}) \\ -sin(\frac{\theta}{2}) & e^{-i\phi}cos(\frac{\theta}{2}) \end{pmatrix}$$

On voit alors que : $\theta' = \theta, \phi' = \pi$ et $\lambda = -\phi - \pi$, autrement dit :

$$P^\dagger = U_3(\theta, \pi, -\phi - \pi)$$

Troisième et dernière étape :

Une fois les matrices de passage calculées, il ne reste plus qu'à mesurer $P^\dagger |\psi\rangle$ dans la base Z :

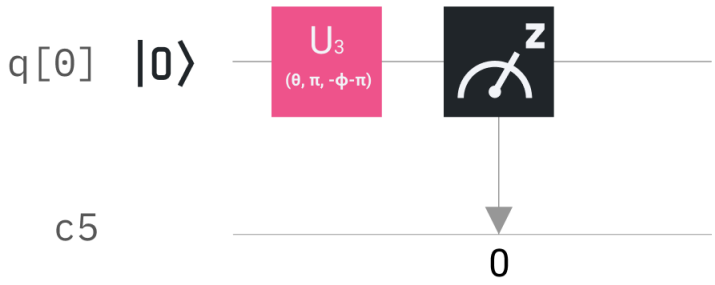


FIGURE 2.3 – Circuit de mesure de $U_3(\theta, \pi, -\phi - \pi)\,|0\rangle$ dans la base Z sur la machine IBM

2.4.2 Exemple de mesures d'états dans une base quelconque

On cherche à mesurer dans la base $\frac{X+Y}{\sqrt{2}}$ les états $|0\rangle$ et $|+\rangle$.
Commençons la démarche pour mesurer $|0\rangle$ dans la base $\mathcal{O} = \frac{X+Y}{\sqrt{2}}$. La direction dans la sphère de Bloch sera $(0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$.
Résolvons le système suivant :

$$\begin{cases} \alpha &= sin(\theta)cos(\phi) \\ \beta &= sin(\theta)sin(\phi) \\ \gamma &= cos(\theta) \end{cases} \Rightarrow \begin{cases} 0 &= \frac{\sqrt{2}}{2}cos(\phi) \\ \frac{\sqrt{2}}{2} &= \frac{\sqrt{2}}{2}sin(\phi) \\ \theta &= \frac{\pi}{4} \end{cases} \Rightarrow \begin{cases} 0 &= cos(\phi) \\ 1 &= sin(\phi) \\ \theta &= \frac{\pi}{4} \end{cases} \Rightarrow \begin{cases} \phi &= \frac{\pi}{2} \\ \theta &= \frac{\pi}{4} \end{cases}$$

D'après le protocole de la partie 2.4.1, on peut directement trouver la matrice conjuguée transposée de la matrice de passage P, ainsi :

$$P^\dagger = U_3(\theta, \pi, -\phi - \pi) = U_3(\frac{\pi}{4}, \pi, -\frac{\pi}{2} - \pi)$$

Enfin, on peut créer le circuit afin de réaliser les mesures :

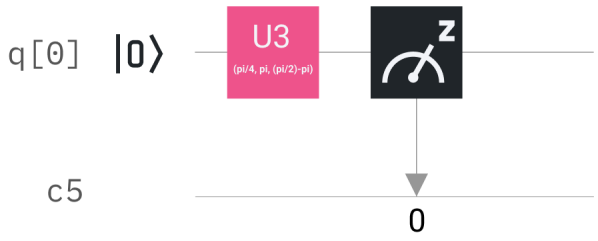


FIGURE 2.4 – Circuit de mesure du qubit $|0\rangle$ dans la base $\frac{X+Y}{\sqrt{2}}$

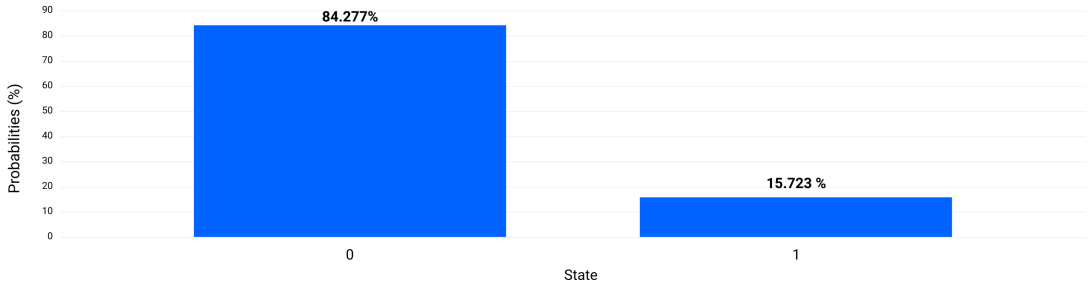


FIGURE 2.5 – Résultats des mesures du qubit $|0\rangle$ dans la base $\frac{X+Y}{\sqrt{2}}$

Finalement pour le qubit dans l'état $|+\rangle$, la matrice de passage est la même que pour le qubit précèdent, il ne reste donc qu'à créer le circuit :

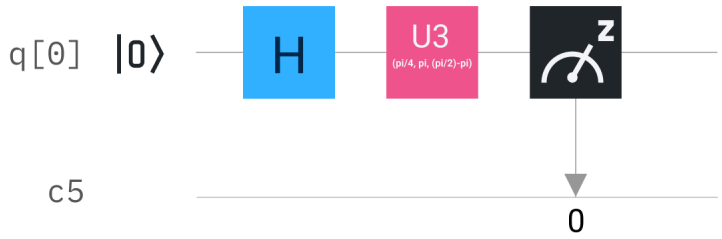


FIGURE 2.6 – Circuit de mesure du qubit $|+\rangle$ dans la base $\frac{X+Y}{\sqrt{2}}$

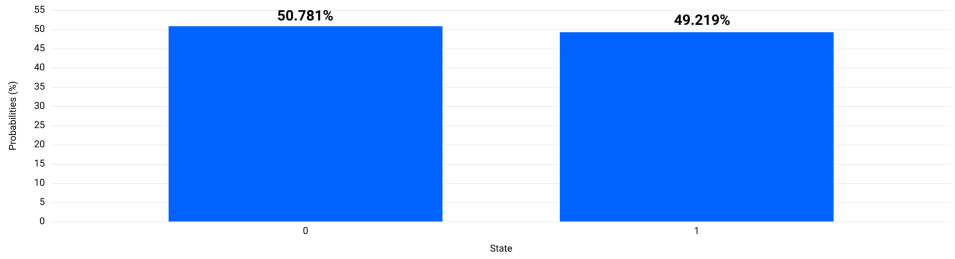


FIGURE 2.7 – Résultats des mesures du qubit $|+\rangle$ dans la base $\frac{X+Y}{\sqrt{2}}$

2.5 Les portes quantiques

Dans la partie 2.4.1 détaillant un protocole de mesure sur la machine d'IBM, nous avons réalisé plusieurs circuits qui contenaient des "blocks" qui sont en fait des **portes quantiques**.
Tout comme le qubit est l'analogue du bit, les portes quantiques sont en fait des "équivalents" aux portes logiques que l'on retrouve dans les ordinateurs classiques. Ces portes permettent de manipuler des qubits et de faire des opérations que l'on ne peut pas faire avec des portes "classiques". Il existe un très grand nombre de portes quantiques, mais nous ne nous attarderons que sur celles qui seront nécessaires pour les expériences et les protocoles que nous allons étudier ensuite.
Chaque porte quantique est représentée par une matrice unitaire.
Rappel partie 2.3 : Une matrice unitaire est une matrice carrée U de taille n à coefficients complexes qui vérifie :

$$U \cdot U^\dagger = U^\dagger \cdot U = I_n$$

Où $U^\dagger$ est la matrice adjointe (conjuguée transposée) de U et I_n la matrice identité de taille n.

Les portes que nous verrons dans ce rapport sont des portes fonctionnant sur des espaces de un ou deux qubits.
Finalement, appliquer une porte à un qubit dans un circuit revient à multiplier l'état du qubit par la matrice représentant la porte en question.

2.5.1 Porte de Hadamard

La porte de Hadamard transforme l'état basique ($|0\rangle$ ou $|1\rangle$) d'un qubit, en état superposé (voir figure 2.8 ci-dessous). Elle représente une rotation de π sur l'axe Z et sur l'axe X sur la sphère de Bloch 2.4.

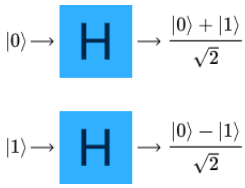


FIGURE 2.8 – porte de Hadamard

Cette porte est représentée par la matrice unitaire : $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

2.5.2 Portes Pauli

Il existe 3 portes Pauli, du nom du physicien Autrichien Wolfgang Ernst Pauli. Ces 3 portes ne s'appliquent qu'à un seul qubit.

La porte Pauli-X

Cette porte peut être considérée comme la porte NOT des portes quantiques car, à un état, elle fait correspondre l'état opposé. Cela équivaut à une rotation de π radians autour de l'axe X de la sphère de Bloch 2.4. Cette porte est représentée par la matrice $X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

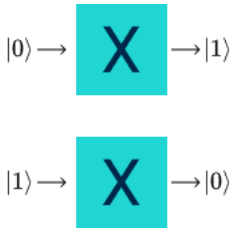


FIGURE 2.9 – Porte Pauli-X

La porte Pauli-Y

Cette porte applique une rotation de π radians autour de l'axe Y, elle est représentée par la matrice $Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ et a comme correspondance : voir figure 2.10.

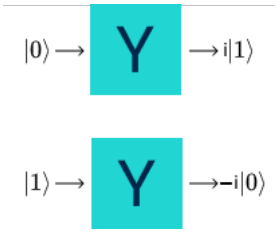


FIGURE 2.10 – Porte Pauli-Y

La porte Pauli-Z

Cette porte est représentée par la matrice $Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Comme pour les deux portes précèdentes, appliquer la porte Z revient à appliquer une rotation de π radians sur l'axe Z. Elle fait correspondre $-|1\rangle$ à $|1\rangle$ et ne change pas $|0\rangle$.

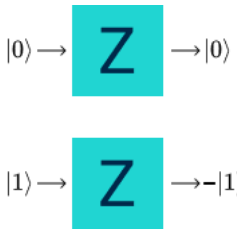


FIGURE 2.11 – Porte Pauli-Z

2.5.3 Porte CNOT ou control NOT

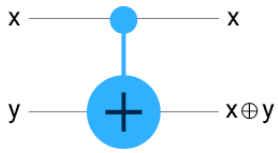


FIGURE 2.12 – Porte CNOT avec $x \oplus y$ l'opérateur booléen XOR

Cette porte agit sur 2 qubits, 1 qubit sert de contrôle, l'autre sera le qubit sur lequel la porte agit. La règle est que l'opération NOT est appliquée au qubit que lorsque le bit de contrôle est dans l'état $|1\rangle$. Cette porte peut être représentée par une matrice de taille 4×4 :

$$CNOT = cX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{pmatrix} \text{ avec } \begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X = \sigma_x$$

Elle fait correspondre à une paire de qubit (x, y), cette paire : $(x, x \oplus y)$, dont on rappelle la table de vérité :

x	y	x⊕y
0	0	0
0	1	1
1	0	1
1	1	0

FIGURE 2.13 – Table de vérité $x \oplus y$

Autrement dit, on peut l'écrire :

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |1\rangle \otimes X\,|0\rangle = |1\rangle \otimes |1\rangle = |11\rangle \\ |11\rangle &\mapsto |1\rangle \otimes X\,|1\rangle = |1\rangle \otimes |0\rangle = |10\rangle \end{aligned}$$

Cette porte est généralement utilisée pour générer des états intriqués.

2.6 L'intrication quantique

Deux particules intriquées sont deux objets quantiques qui ont la particularité de former un seul et même système ; ce qui a pour conséquence que la mesure de l'état d'un des objets influence **instantanément** la mesure de l'état du deuxième objet, autrement dit, connaître l'état d'un objet nous permet d'en déduire l'état du deuxième. Nous verrons que cette propriété des objets quantiques peut être utilisée dans certains protocoles de cryptographie quantique dont nous parlerons dans le chapitre 2.
Prenons l'exemple de l'état EPR :

$$|\phi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

On a dit précédemment que la mesure d'un des deux objets (ici des qubits) influencera directement la mesure de l'état du deuxième qubit. Imaginons maintenant qu'un des qubits du système soit envoyé à Alice et l'autre à Bob et que les deux personnes soient éloignées de plusieurs milliers de kilomètres. Lorsqu'Alice mesure l'état de son qubit, si elle obtient 0, l'axiome 3 sur l'état des mesures nous dit que l'état de son qubit va être directement projeté sur le seul résultat possible, ici : $|\phi_{EPR}\rangle \rightsquigarrow |00\rangle$, ainsi Bob mesurera l'état de son qubit et obtiendra 0 avec une probabilité de 1. Le raisonnement pour la mesure de l'état 1 est le même.

L'intrication quantique entre 2 qubits peut être générée sur la machine d'IBM en utilisant une porte Hadamard ainsi qu'une porte CNOT de cette manière :

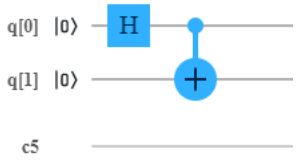


FIGURE 2.14 – Création d'un état intriqué

Calculons l'équivalent "mathématique" de ce circuit. Soit q[0] et q[1] les deux qubits du circuit 2.14 ci-dessus.
Ces deux qubits forment un système : $|00\rangle = |0\rangle \otimes |0\rangle$.
Le circuit consiste à appliquer la matrice unitaire H à q[0] :

$$H \cdot |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

On applique ensuite la porte CNOT au système :

$$CNOT(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle)$$

Ce qui donne alors :

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes X \cdot |0\rangle)$$

On retrouve finalement l'état EPR :

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi_{EPR}\rangle$$

2.7 Les inégalités de Bell

2.7.1 Théorie

Les inégalités de Bell sont un ensemble de relations que doivent respecter les mesures de deux objets quantiques intriqués sous l'hypothèse d'une théorie **déterministe locale** à **variables cachées**.
Autrement dit, suite à un désaccord dans la communauté scientifique, certains physiciens, dont Albert Einstein, Boris Podolsky et Nathan Rosen (d'où le nom de l'état de deux qubits intriqués EPR), pensaient qu'il était impossible qu'une théorie **probabiliste** puisse expliquer la mécanique quantique. Ils introduirent alors le principe de **variables cachées**, des paramètres physiques hypothétiques pas encore découverts, qui expliqueraient tout ce qu'on considérait comme "dû au hasard" en mécanique quantique. En résumé, ils pensaient que la théorie de la mécanique quantique était incomplète.
Le terme *local*, indique ici qu'il ne peut pas y avoir d'interaction entre deux systèmes distants l'un de l'autre.
Bell démontra alors que pour que le réalisme local soit respecté, il fallait qu'une contrainte soit respectée sur les mesures des objets quantiques intriqués. Ici, nous utiliserons l'inégalité de Bell-CHSH [2] :

$$|C| \leq 2$$

Avec

$$C = \langle AB \rangle + \langle A'B \rangle + \langle AB' \rangle - \langle A'B' \rangle \tag{2.4}$$

où $\langle AB \rangle$ est l'espérance du produit des résultats des mesures de l'état du premier qubit mesuré dans la base A par l'état du deuxième qubit mesuré dans la base B.
Autrement dit :

$$\langle AB \rangle = P_{00}(A,B) + P_{11}(A,B) - P_{01}(A,B) - P_{10}(A,B)$$

On peut définir $\langle A'B \rangle, \langle AB' \rangle$ et $\langle A'B' \rangle$ de la même manière.

2. John Clauser, Michael Horne, Abner Shimony, and Richard Holt

Soit $|\phi_{EPR}\rangle$ le système de deux qubits :

$$|\phi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.5}$$

Soit A, A', B et B', quatre observables :

$$A = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$A' = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$B = \frac{Z+X}{\sqrt{2}} = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$B' = \frac{Z-X}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

On cherche à calculer la quantité C théorique, afin de vérifier que l'inégalité Bell-CHSH est bien violée, et donc que le système de deux qubits EPR n'est pas régit par une théorie déterministe locale à variables cachées.
Calculons la valeur de C théorique :

$$\begin{aligned}
\langle AB \rangle &= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \bigotimes \begin{pmatrix} 1\sqrt{2} & 1\sqrt{2} \\ 1\sqrt{2} & -1\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1\sqrt{2} & 1\sqrt{2} & 0 & 0 \\ 1\sqrt{2} & -1\sqrt{2} & 0 & 0 \\ 0 & 0 & -1\sqrt{2} & -1\sqrt{2} \\ 0 & 0 & -1\sqrt{2} & 1\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \frac{\sqrt{2}}{2}
\end{aligned}$$

$$\begin{aligned}
\langle AB' \rangle &= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \bigotimes \begin{pmatrix} 1\sqrt{2} & -1\sqrt{2} \\ -1\sqrt{2} & -1\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1\sqrt{2} & -1\sqrt{2} & 0 & 0 \\ -1\sqrt{2} & -1\sqrt{2} & 0 & 0 \\ 0 & 0 & -1\sqrt{2} & 1\sqrt{2} \\ 0 & 0 & 1\sqrt{2} & 1\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \frac{\sqrt{2}}{2}
\end{aligned}$$

$$\langle A'B\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \bigotimes \begin{pmatrix} 1\sqrt{2} & 1\sqrt{2} \\ 1\sqrt{2} & -1\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1\sqrt{2} & 1\sqrt{2} \\ 0 & 0 & 1\sqrt{2} & -1\sqrt{2} \\ 1\sqrt{2} & 1\sqrt{2} & 0 & 0 \\ 1\sqrt{2} & -1\sqrt{2} & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$= \frac{\sqrt{2}}{2}$$

$$\langle A'B'\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \bigotimes \begin{pmatrix} 1\sqrt{2} & -1\sqrt{2} \\ -1\sqrt{2} & -1\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1\sqrt{2} & -1\sqrt{2} \\ 0 & 0 & -1\sqrt{2} & -1\sqrt{2} \\ 1\sqrt{2} & -1\sqrt{2} & 0 & 0 \\ -1\sqrt{2} & -1\sqrt{2} & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$= -\frac{\sqrt{2}}{2}$$

Finalement, on obtient :

$$C = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} - (-\frac{\sqrt{2}}{2}) = 2\sqrt{2}$$

Suite au calcul théorique, on voit alors que $|C| > 2$, ainsi on peut affirmer que les résultats des mesures des objets quantiques intriqués ne peuvent pas être déterminés à l'aide de la théorie des variables cachées locales. Autrement dit, il est impossible de donner les résultats des mesures dans les expériences de type EPR à l'aide d'une théorie déterministe locale.

Le théorème nous sera utile dans le protocole E91 afin de vérifier qu'un espion n'a pas modifié l'état des qubits transmis.

2.7.2 Vérification expérimentale

Nous pouvons vérifier la valeur de C en réalisant des mesures grâce à l'ordinateur quantique d'IBM : La première étape pour réaliser les mesures est de chercher la matrice de passage de la base Z aux bases A, A', B et B'.
Rappelons que :

$$\begin{aligned} A &= Z \\ A' &= X \\ B &= \frac{Z+X}{\sqrt{2}} = H \\ B' &= \frac{Z-X}{\sqrt{2}} \end{aligned}$$

Ainsi il nous faut trouver la matrice de passage de :

- La base **Z** vers la base **X**, c'est à dire résoudre le système suivant :

$$\begin{cases} \alpha &= sin(\theta)cos(\phi) \\ \beta &= sin(\theta)sin(\phi) \\ \gamma &= cos(\theta) \end{cases}$$

  Sachant qu'ici l'observable $\mathcal{O} = \alpha X + \beta Y + \gamma Z = 1X + 0Y + 0Z$.
  Le système est alors le suivant :

$$\begin{cases} 1 &= sin(\theta)cos(\phi) \\ 0 &= sin(\theta)sin(\phi) \\ 0 &= cos(\theta) \end{cases} \Rightarrow \begin{cases} 1 &= cos(\phi) \\ 0 &= sin(\phi) \\ \theta &= \frac{\pi}{2} \end{cases} \Rightarrow \begin{cases} \phi &= 0 \\ \phi &= 0 \\ \theta &= \frac{\pi}{2} \end{cases}$$

  Ainsi comme vu dans la partie sur la sphère de Bloch, nous pouvons noter la matrice de passage :

$$P = U_3(\theta = \frac{\pi}{2}, \phi = 0, \lambda = 0) = \begin{pmatrix} cos(\frac{\pi}{4}) & -sin(\frac{\pi}{4}) \\ sin(\frac{\pi}{4}) & cos(\frac{\pi}{4}) \end{pmatrix}$$

  Et ainsi définir et calculer sa conjuguée transposée que l'on multipliera par $|\phi_{EPR}\rangle$ avant d'appliquer la mesure :

$$P^\dagger = U_3(\frac{\pi}{2}, \pi, -\pi) = \begin{pmatrix} cos(\frac{\pi}{4}) & sin(\frac{\pi}{4}) \\ -sin(\frac{\pi}{4}) & cos(\frac{\pi}{4}) \end{pmatrix}$$

- La base **Z** vers la base $\frac{Z+X}{\sqrt{2}}$, on procède de la même manière que précédemment et on obtient :

$$P^\dagger = U_3(\frac{\pi}{4}, \pi, -\pi) = \begin{pmatrix} cos(\frac{\pi}{8}) & sin(\frac{\pi}{8}) \\ -sin(\frac{\pi}{8}) & cos(\frac{\pi}{8}) \end{pmatrix}$$

- La base **Z** vers la base $\frac{Z-X}{\sqrt{2}}$, on obtient :

$$P^\dagger = U_3(\frac{\pi}{4}, \pi, -2\pi) = \begin{pmatrix} cos(\frac{\pi}{8}) & e^{-i\pi}sin(\frac{\pi}{8}) \\ -sin(\frac{\pi}{8}) & e^{-i\pi}cos(\frac{\pi}{8}) \end{pmatrix}$$

Mesurons maintenant l'état $|\phi_{EPR}\rangle$ dans chacune des bases afin de trouver les valeurs de : $\langle AB\rangle, \langle A'B\rangle, \langle AB'\rangle$ et $\langle A'B'\rangle$

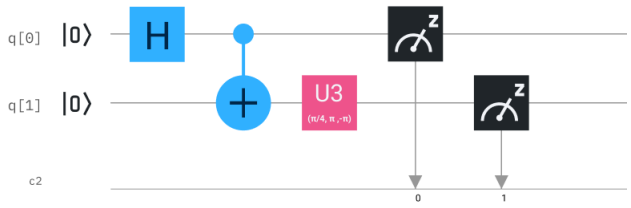


FIGURE 2.15 – Circuit de mesure dans AB du système

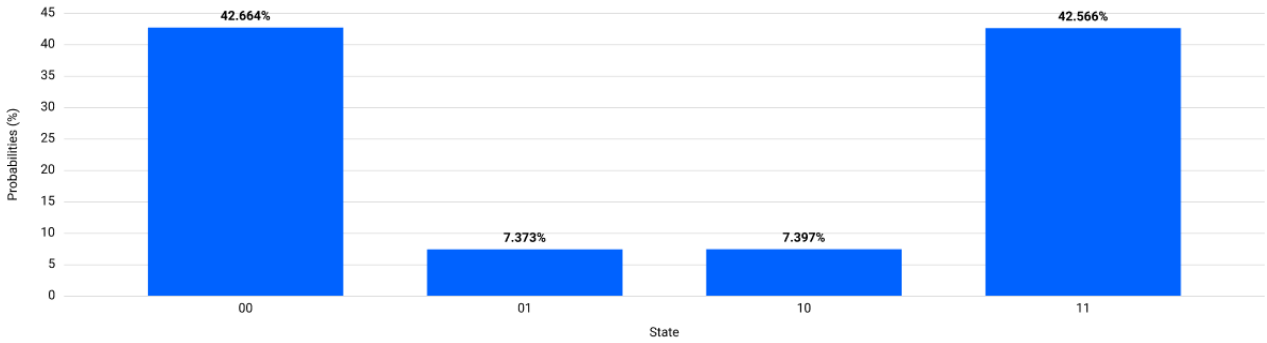


FIGURE 2.16 – Résultats de la mesure du système dans AB

$$\begin{aligned}\langle AB\rangle &= 0.42664 - 0.07373 - 0.07397 + 0.42566 \\ &= 0.7046\end{aligned}$$

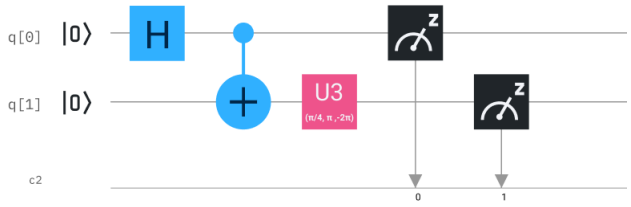


FIGURE 2.17 – Circuit de mesure dans AB' du système

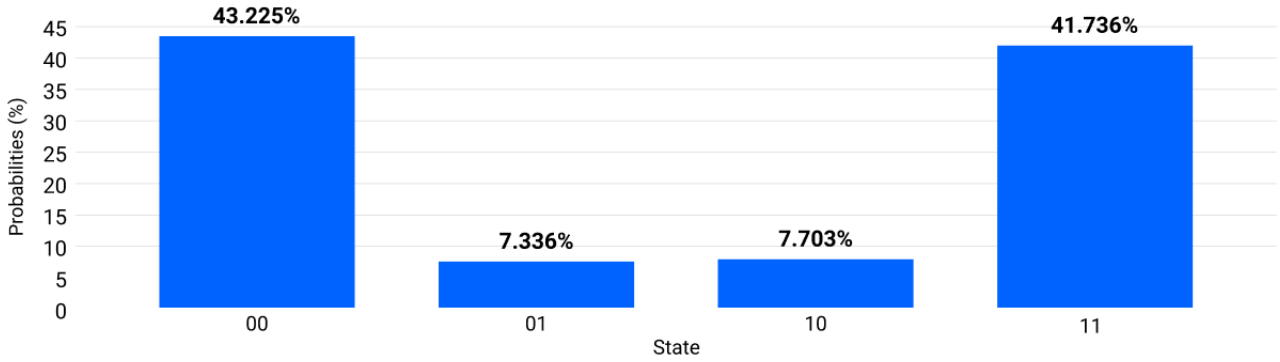


FIGURE 2.18 – Résultats de la mesure du système dans AB'

$$\begin{aligned}\langle AB' \rangle &= 0.43225 - 0.07336 - 0.07703 + 0.41736 \\ &= 0.69922\end{aligned}$$

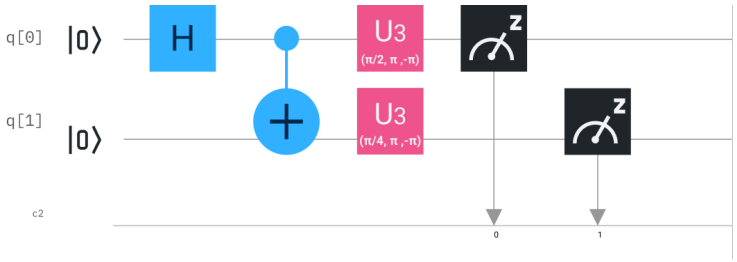


FIGURE 2.19 – Circuit de mesure dans A'B du système

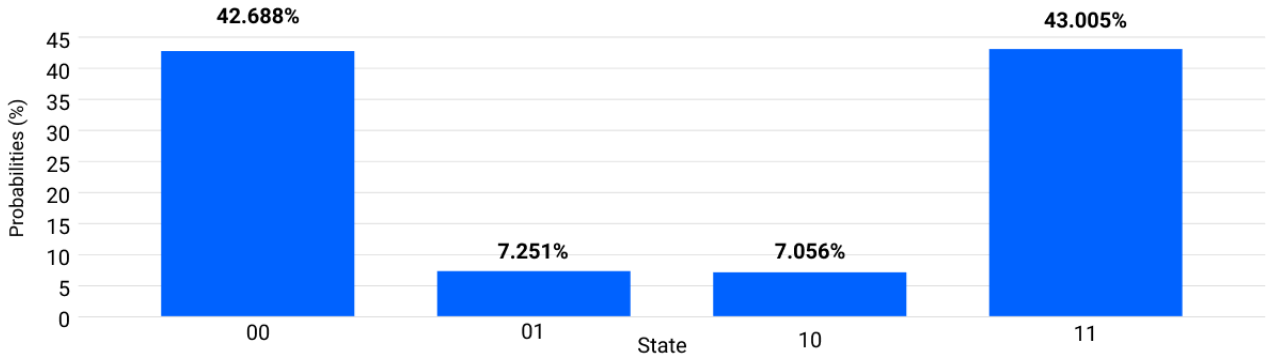


FIGURE 2.20 – Résultats de la mesure du système dans A'B

$$\begin{aligned}\langle A'B\rangle &= 0.42688 - 0.07251 - 0.07056 + 0.43005 \\ &= 0.71386\end{aligned}$$

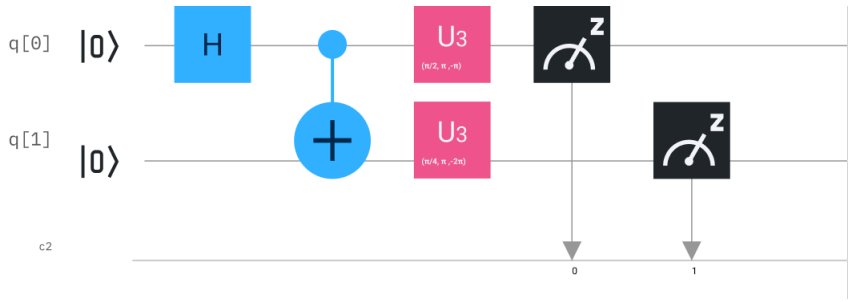


FIGURE 2.21 – Circuit de mesure dans A'B' du système

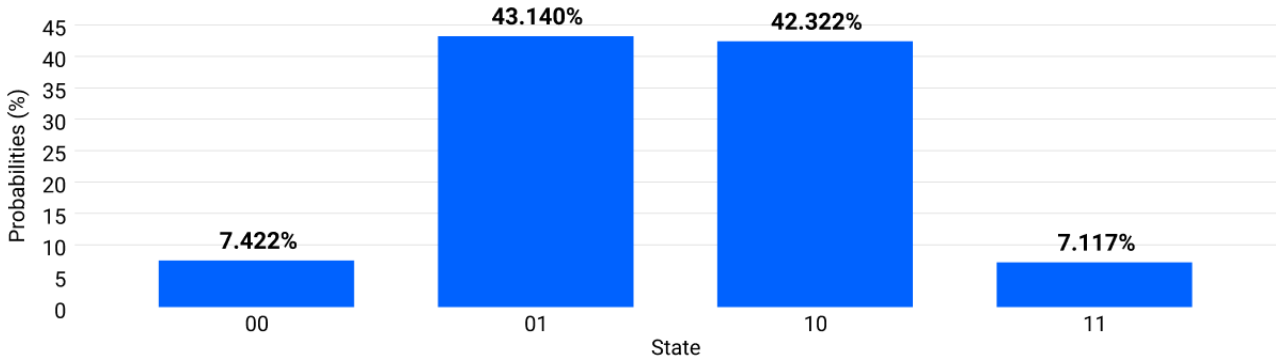


FIGURE 2.22 – Résultats de la mesure du système dans A'B'

$$\begin{aligned}\langle A'B'\rangle &= 0.07422 - 0.43140 - 0.42322 + 0.7117 \\ &= -0.0687\end{aligned}$$

On peut finalement calculer la valeur de $|C|$:

$$|C| = |0.7046 + 0.69922 + 0.71386 - (-0.0687)| = 2.18638 > 2$$

Ce résultat est cohérent avec ce que nous avons vérifié théoriquement dans la partie 2.7.1. On se doit alors de rappeler que la mesure de l'état des qubits est probabiliste, lorsque nous effectuons une expérience, la machine réalise plusieurs essais afin d'avoir des résultats statistiques les plus précis possibles. Dans notre cas, toutes les mesures sont répétées 8192 fois. Bien qu'un grand nombre d'essais soit réalisé, l'éventualité que de nombreuses erreurs de mesure faussent les statistiques ne doit pas être négligée.

Chapitre 3

Protocoles de cryptographie quantique

3.1 Protocole BB84

3.1.1 Principe

Le protocole BB84 est un protocole de cryptographie quantique développé par Charles Benett et Gilles Brassard en 1984. Il est un des premiers de ce genre et permet d'échanger une clé de cryptage pour réaliser de la **cryptographie symétrique**. Le problème de ce type de cryptographie étant de faire en sorte que les interlocuteurs connaissent la clé pour crypter et décrypter des données, il est nécessaire de trouver un moyen sûr d'échanger la clé sans qu'elle ne soit utilisable par une personne tierce qui chercherait à espionner l'échange. C'est à ce moment précis que le protocole BB84 intervient.

3.1.2 Réalisation

Tim et Elodie sont deux interlocuteurs. Ils décident d'utiliser un chiffrement symétrique et cherchent à s'échanger la clé de cryptage de manière sécurisée, que personne ne puisse connaître la clé de cryptage. Tim et Elodie peuvent :

- S'appeler et échanger des informations (mais ce n'est pas sécurisé)
- Encoder et décoder des bits à l'aide de qubit projeté dans une certaine base

Ils cherchent à se communiquer une chaîne de bits, composée de 0 et de 1, codée à l'aide de qubits.

Protocole d'échange de la clé :

1. Tim génère aléatoirement la chaîne de taille N.
2. Tim encode chaque bit en qubit en choisissant aléatoirement une base parmi deux : La base Standard ($|0\rangle, |1\rangle$) ou la base de Hadamard ($|+\rangle, |-\rangle$). Les bases correspondent à des directions sur la Sphère de Bloch 2.4.
3. Tim envoie l'ensemble des qubits à Elodie.

4. Elodie reçoit les qubits et les mesure avec une des deux bases vues précédemment aléatoirement. Elle note les résultats.
5. Une fois que les qubits ont été réceptionnés, Elodie et Tim s'appellent. Pour chaque qubits, ils se communiquent la base qui a été utilisée pour la mesure du qubit en question. Finalement, ils ne conservent que les qubits pour lesquels ils ont utilisé la même base pour le cryptage et la mesure. Une fois décodé, ils disposent tous les deux de la clé de cryptage.

Exemple d'échange d'une clé :

Reprenons l'échange de la clé avec un exemple.
Tim et Elodie cherchent à se communiquer une clé de cryptage pour échanger des informations.
Tout d'abord, Tim génère une chaîne de caractères de 0 et de 1 de taille $N = 12$.
Voici la chaîne de caractères : $1011 \quad 0110 \quad 1010$.
Ensuite, pour chaque bit, Tim choisi parmi les deux bases pour le coder. On rappelle que :

Dans la base **Standard** S :
$0 \rightarrow |0\rangle$
$1 \rightarrow |1\rangle$
Dans la base **Hadamard** H :
$0 \rightarrow |+\rangle$
$1 \rightarrow |-\rangle$

D'où, le choix des bases aléatoire est : $SSHH \quad SHSH \quad SHHH$
Finalement, on obtient le tableau suivant dans lequel on trouve la chaîne de bits, la base utilisée pour coder le bit et son "équivalent" en qubit.

Chaîne de bits	$1011 \quad 0110 \quad 1010$
Bases	$SSHH \quad SHSH \quad SHHH$
Qubits	$\|1\rangle\|0\rangle\|-\rangle\|-\rangle \quad \|0\rangle\|-\rangle\|1\rangle\|+\rangle \quad \|1\rangle\|+\rangle\|-\rangle\|+\rangle$

Tim envoie donc la liste de qubits à Elodie, qui va réceptionner chaque qubit en utilisant une base au hasard.
Elle utilise cette combinaison de bases : $SHHS \quad SSSH \quad SHSH$
Dans le cas où la base choisie par Elodie est la **même** que celle choisie par Tim pour envoyer le qubit en question, la probabilité que le qubit soit projeté sur le même état que celui envoyé est de 1. Sinon, Elodie a 50% de chance de tomber sur le même état qu'à l'envoi et 50% de chance que l'état ne soit pas le même.
Ainsi, dans le cas où Tim a envoyé un qubit $|1\rangle$ dans la base standard, si Elodie mesure l'état du qubit dans la base standard, elle obtiendra $|1\rangle$, autrement dans le cas où elle mesure dans la base de Hadamard, elle obtiendra $|0\rangle$ ou $|1\rangle$ avec une probabilité de 50% pour chaque état. Le principe est le même, peu importe l'état du qubit à l'envoi et la base choisie.
Finalement, Elodie mesure :

Chaîne de bits	1	0	1	1	0	1	1	0	1	0	1	0
Bases de Tim	S	S	H	H	S	H	S	H	S	H	H	H
Qubits envoyés	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$
Bases d'Elodie	S	H	H	S	S	S	S	H	S	H	S	H
Qubits mesurés	$\|1\rangle$	$\|+\rangle$ ou $\|-\rangle$	$\|-\rangle$	$\|1\rangle$ ou $\|0\rangle$	$\|0\rangle$	$\|1\rangle$ ou $\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$ ou $\|0\rangle$	$\|+\rangle$

Suite à leur appel, Elodie a révélé à Tim quelles bases elle a utilisé pour la mesure. Ils ne conservent que les qubits pour lesquels ils ont utilisé la même base afin d'avoir une probabilité de 100% de mesurer le même état pour un même qubit.
La **clé** de cryptage sera dans notre cas : 11010100

3.1.3 Cas où un espion observe

Nous allons nous intéresser maintenant au cas où un espion chercherait à intercepter la clé pendant le transfert des qubits de Tim vers Elodie. Si un espion cherche à observer l'échange, la mesure va modifier l'état des qubits mesurés (d'après l'axiome 3 dans la partie sur les bases de l'informatique quantique (2.3), l'état du qubit mesuré va être projeté sur un des états de base avec une probabilité de 50%). Une fois que Tim et Elodie auront échangé leurs listes de bases dans lesquelles ils ont mesuré l'état de leurs qubits, ils trouveront des incohérences (pas la même mesure pour une même base par exemple) et pourront conclure que la transmission de leur clé n'est probablement pas sécurisée. Dans ce cas, la clé est abandonnée.

Calcul de la probabilité que l'espion ne soit pas détecté

Calculons la probabilité qu'un espion mesure l'état d'un qubit en passant inaperçu.
Premièrement, considérons que l'espion choisit une base pour mesurer l'état du qubit, disons la base **Hadamard**. Si Tim envoie le qubit dans la base Hadamard, alors l'espion mesurera le même état que Tim avec une probabilité $p = 1$.
Si Tim envoie le qubit dans la base Standard, l'espion mesurera l'état du qubit avec une probabilité $p = 0.5$
Mais, nous savons que Tim choisit la base dans laquelle il envoie le qubit avec une probabilité de 0.5, ainsi, on peut poser ces trois événements :

- A : "Tim choisi la base Standard S"
- B : "Tim choisi la base Hadamard H"
- E : "L'espion mesure le même état que celui envoyé par Tim"

On peut alors affirmer : $P(A) = P(B) = P_A(E) = \frac{1}{2}$ et $P_B(E) = 1$
De plus, $P(E) = P(E \cap A) + P(E \cap B)$
Ainsi, $P(E) = P(A) \cdot P_A(E) + P(B) \cdot P_B(E)$
Par conséquent, $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot 1 = \frac{3}{4}$
Finalement, on peut affirmer que lors du transfert d'un qubit, l'espion a **3 chances sur 4** d'intercepter le qubit sans changer son état.
Maintenant, si on décide d'échanger n qubits, la probabilité que l'espion intercepte le qubit sans changer son état diminue très vite car elle vaut $(\frac{3}{4})^n$. Par exemple, à partir de 10 qubits échangés, la probabilité est : $(\frac{3}{4})^{10} = 0.0563135147$

3.2 Protocole E91

3.2.1 Principe

Le protocole E91 est un protocole de cryptographie quantique reposant sur le principe d'intrication quantique. Il a été développé par Artur Ekert [1] en 1991 et permet, comme le protocole BB84, d'échanger une clé afin de crypter des échanges d'informations.

3.2.2 Réalisation

Protocole

1. Une source émet des paires de qubits **intriqués**. L'état du système peut être noté de la façon suivante :
$$|\phi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$$
Alice et Bob sont deux personnes qui cherchent à se communiquer une clé afin de crypter leurs communications.
2. Un qubit de la paire est envoyé à Alice et l'autre à Bob. Ils disposent tous les deux de **trois** détecteurs.
Alice mesure les qubits qu'elle reçoit selon 3 observables différents correspondants à des orientations dans la sphère de Bloch 2.4. On note A_i, avec $i \in \{1, 2, 3\}$ le vecteur représentant l'orientation des détecteurs par rapport à l'axe z dans le plan z-x.
On peut décrire les A_i par des angles :
$$\theta_1^A = 0 \qquad \theta_2^A = \frac{\pi}{4} \qquad \theta_3^A = \frac{\pi}{2}$$

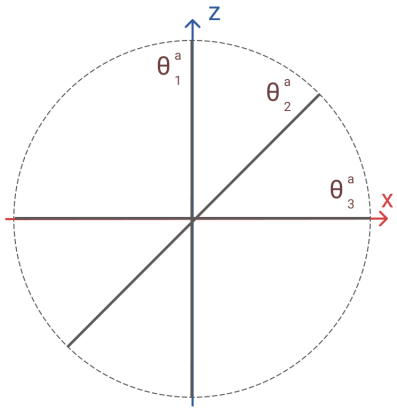


FIGURE 3.1 – Illustration des bases/orientations utilisées par Alice

1. Professeur de physique quantique à l'Université de Oxford

Autrement dit, en utilisant les notations de la sphère de Bloch 2.4, on obtient :

$$A_1 = Z \qquad A_2 = \frac{X+Z}{\sqrt{2}} \qquad A_3 = X$$

On peut aussi définir les vecteurs représentant l'orientation des détecteurs de Bob. On note B_j, avec $j \in \{1,2,3\}$, le vecteur représentant l'orientation des détecteurs de Bob. On peut décrire les B_j avec des angles, comme pour Alice :

$$\theta_1^B = \frac{\pi}{4} \qquad \theta_2^B = \frac{\pi}{2} \qquad \theta_3^B = \frac{3\pi}{4}$$

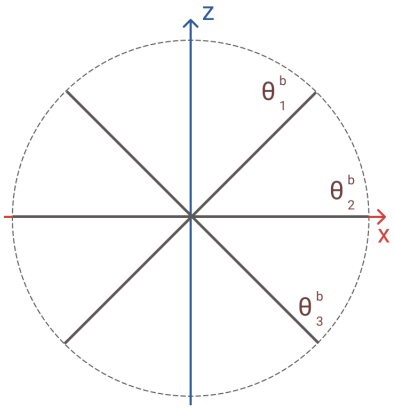


FIGURE 3.2 – Illustration des bases/orientations utilisées par Bob

Ce qui revient à écrire B_j sous la forme suivante :

$$B_1 = \frac{X+Z}{\sqrt{2}} \qquad B_2 = X \qquad B_3 = \frac{X-Z}{\sqrt{2}}$$

En définissant ces orientations dans la sphère de Bloch, nous pourrons ensuite vérifier si les inégalités de Bell sont violées ou non et donc affirmer ou pas que l'échange de la clé a été espionné.

3. Mais avant de vérifier cela, Alice et Bob vont mesurer chaque qubit reçu dans une direction choisie **aléatoirement** : Alice choisit entre a_1, a_2 et a_3, Bob choisit entre b_1, b_2 et b_3.
   Une fois la transmission des qubits et les mesures effectuées, Alice et Bob peuvent se contacter (par un moyen «publique») afin de s'échanger les directions utilisées pour les mesures.
   Ils séparent alors les mesures en deux groupes :
   - Le premier est constitué des mesures effectuées dans des bases **différentes**.
   - Le second est constitué des celles effectuées dans la **même** base.

   Remarque : Ils ne conservent aucune mesure où l'un ou les deux n'ont pas réussi à mesurer la particule.

4. La prochaine étape consiste à révéler les résultats du 1^{er} groupe de mesures (celui où les orientations étaient différentes) . Cela va permettre de vérifier que l'inégalité CHSH n'est pas vérifiée, ce qui sera une preuve que le théorème de Bell est bien violé. Autrement dit, les valeurs mesurées du groupe 1 vont nous permettre de vérifier que $|C| > 2$, avec :

$$C = \langle A_1 B_1 \rangle + \langle A_3 B_1 \rangle - \langle A_1 B_3 \rangle + \langle A_3 B_3 \rangle$$

Où $\langle A_i, B_j \rangle$ est l'espérance du résultat de la mesure lorsque l'état du qubit d'Alice est mesuré dans la base A_i et l'état de celui de Bob dans la base B_j.
Si $|C| \leq 2$, l'inégalité CHSH n'est pas violée ; Les qubits ont donc été perturbés directement ou indirectement et donc que l'échange a probablement été espionné.
Ainsi, dans le cas ou $C < 2$, ils peuvent affirmer que personne n'a espionné la transmission.

5. La dernière étape est simplement la récupération de la clé. Sachant qu'ils n'ont pas été espionnés, ils conservent alors les résultats des mesures où les orientations des détecteurs étaient les mêmes. Puisque la source émet des paires de photons intriqués, alors ils obtiendront tous les deux les mêmes résultats pour chaque état mesuré (voir 2.6).

3.3 Réalisation du protocole BB84 sur la machine d'IBM

Dans cette section du rapport, nous allons reproduire le protocole BB84 sur la machine d'IBM [3] expliqué dans la section précédente 3.1.2. Nous allons donc simuler un échange de qubit entre Tim et Elodie. Nous reprendrons les mêmes valeurs que dans l'exemple théorique. Voici le tableau montrant la chaîne de qubit qu'ils cherchent à se communiquer ainsi que les bases dans lesquelles ils ont mesuré chaque qubit :

Chaîne de bits	1	0	1	1	0	1	1	0	1	0	1	0
Bases de Tim	S	S	H	H	S	H	S	H	S	H	H	H
Qubits envoyés	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$
Bases d'Elodie	S	H	H	S	S	S	S	H	S	H	S	H
Qubits mesurés	$\|1\rangle$	$\|+\rangle$ ou $\|-\rangle$	$\|-\rangle$	$\|1\rangle$ ou $\|0\rangle$	$\|0\rangle$	$\|1\rangle$ ou $\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$ ou $\|0\rangle$	$\|+\rangle$

On rappelle que S est la base **S**tandard $(|0\rangle, |1\rangle)$ et H la base **H**adamard $(|+\rangle, |-\rangle)$.

Nous pouvons ainsi réaliser le circuit suivant représentant l'échange de qubits :

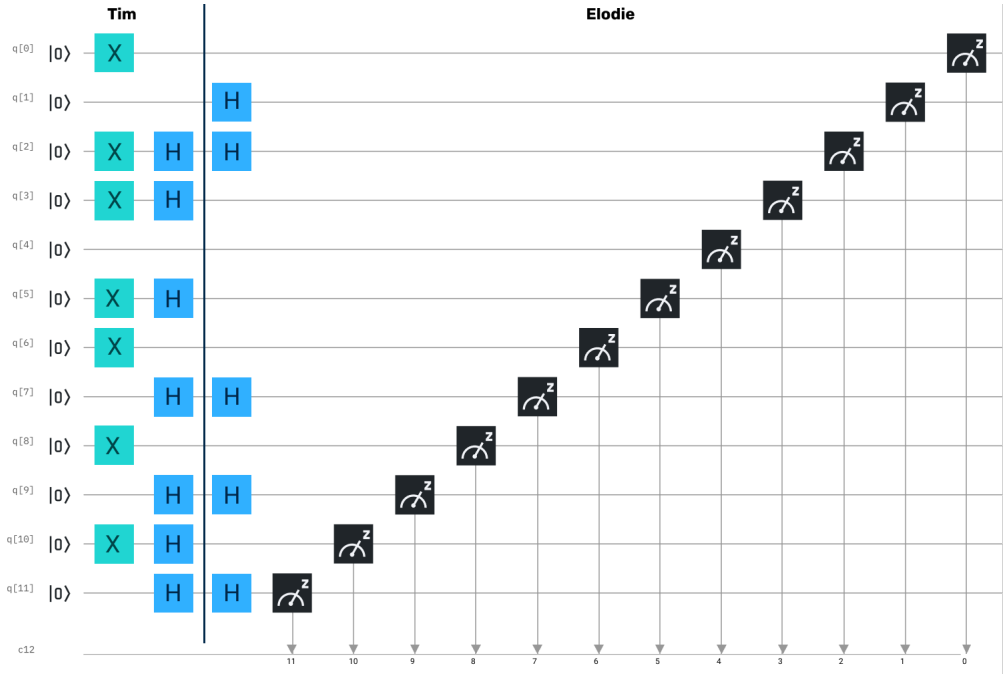


FIGURE 3.3 – Circuit quantique représentant la transmission des qubits de Tim vers Elodie

Ici, la porte X permet de passer d'un état à son opposé. La porte H permet de transformer l'état $|0\rangle$ (resp. $|1\rangle$) en état $|+\rangle$ (resp. $|-\rangle$) et inversement.

On obtient les résultats suivants :

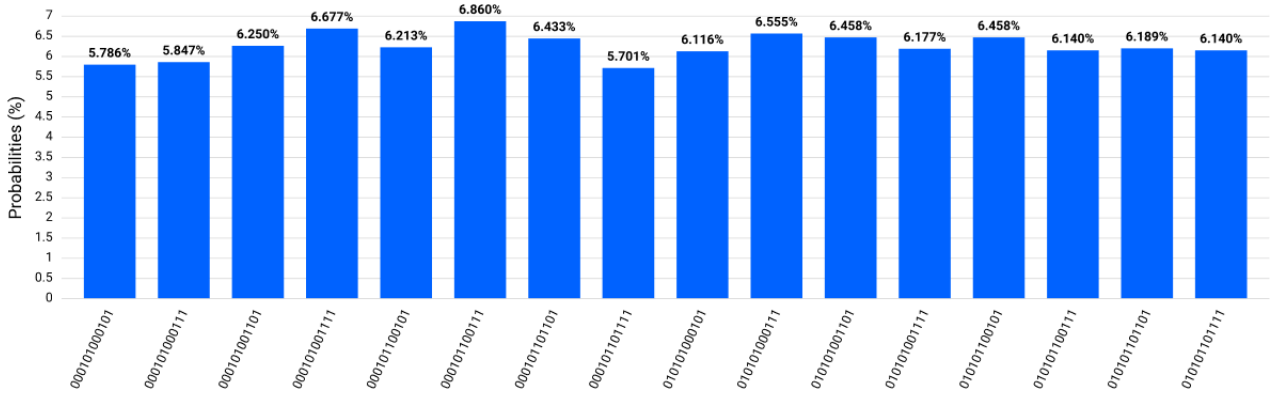


FIGURE 3.4 – Résultat obtenu à l'aide de l'ordinateur quantique d'IBM en effectuant 8192 essais

Nous pouvons ensuite dresser un tableau avec les probabilités par qubit :

Qubits	q[0], q[2], q[7], q[9]	q[1]	q[3]	q[4], q[8], q[9], q[11]	q[5]	q[10]
Probabilité d'obtenir 1	100%	50.097%	50.025%	0%	50.134%	50.233%
Probabilité d'obtenir 0	0%	49.903%	49.975%	100%	49.866%	49.767%

En comparant ce tableau avec le précèdent 3.3, on voit que les qubits pour lesquels Tim et Alice n'ont pas choisi la même base (q[1], q[3], q[5] et q[10]) ont une probabilité d'environ 50% d'être dans l'état $|0\rangle$ (respectivement $|+\rangle$) et d'environ 50% d'être dans l'état $|1\rangle$ (respectivement $|-\rangle$). Ainsi, on remarque que nous sommes en effet très proche de la théorie en utilisant cette machine.

L'espion

Essayons maintenant d'ajouter un espion entre Tim et Elodie :

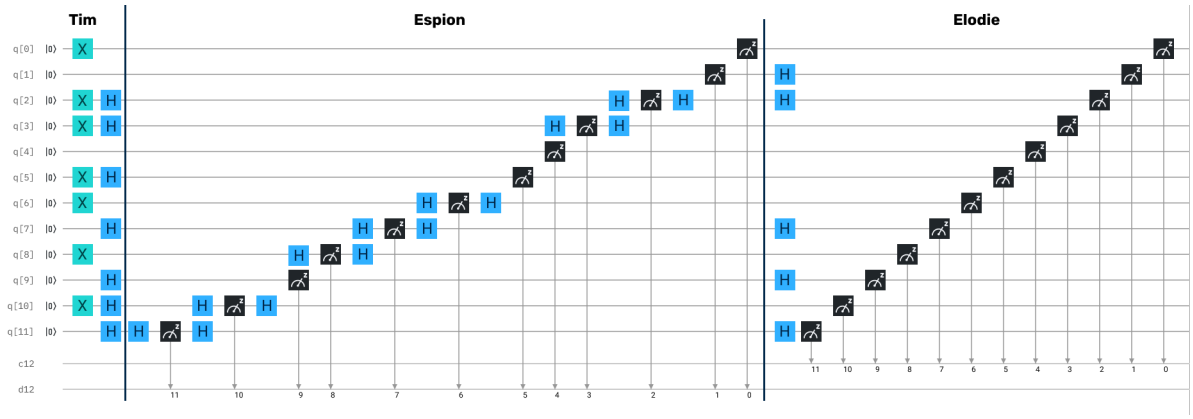


FIGURE 3.5 – Circuit de transfert de qubits de Tim vers Elodie avec un espion observant le transfert

Nous avons vu dans la partie théorique 3.1.3 que la probabilité que l'espion observe un qubit envoyé par Tim sans perturber le protocole est de $\frac{3}{4}$.
Dans cet exemple on peut voir que l'espion a choisi la même base que Tim et Elodie pour 5 qubits sur 8 (nous ne considérons que les qubits pour lesquels Tim et Elodie ont utilisé les mêmes bases), voici la liste : q[0], q[2], q[4], q[7], q[11]. Pour les autres qubits, il n'a pas la même base.

Théoriquement, la probabilité qu'il ait choisi la même base que Tim et qu'il ne modifie pas l'état des qubits pour les 12 qubits est : $(\frac{3}{4})^{12} = 0.031676352$.

3.4 Réalisation du protocole E91 sur la machine d'IBM

Pour la réalisation du protocole E91 sur la machine d'IBM, nous simulerons l'envoi de seulement 6 qubits à Alice et 6 qubits à Bob. Le circuit permettant de modéliser la situation est le suivant :

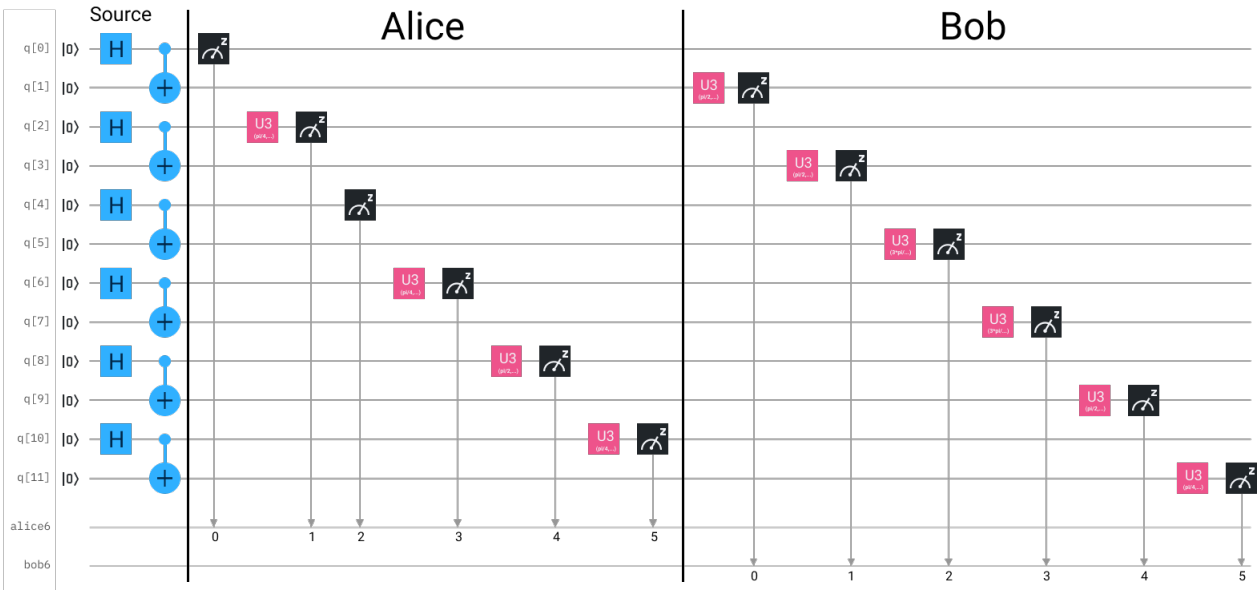


FIGURE 3.6 – Circuit réalisant le protocole E91 sur la machine quantique d'IBM

La source émet des paires de qubits intriqués :

$$|\phi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Voici la liste des directions choisies aléatoirement par Alice et par Bob afin de mesurer l'état des qubits qu'ils reçoivent ainsi que les qubits émis par la source (avant qu'ils ne soient divisés en deux qubits intriqués) :

Qubit	q[0]	q[1]	q[2]	q[3]	q[4]	q[5]
Direction de mesure de Alice	A_1	A_3	A_1	A_3	A_3	A_2
Direction de mesure de Bob	B_1	B_1	B_3	B_3	B_2	B_1

On voit ici que les qubits q[4] et q[5] ont été mesurés dans les **mêmes** directions, ainsi Alice et Bob pourront se servir des résultats des mesures de ces deux qubits pour obtenir leur clé après avoir vérifié que l'inégalité CHSH a bien été violée ($|C| > 2$).

Suite à la mesure des qubits dans les directions différentes notées dans le tableau ci dessus 3.4, on obtient un grand nombre de résultats que nous allons formater et trier à l'aide de l'algorithme (voir annexe A).

Celui ci permet de calculer les probabilités d'obtenir $|00\rangle$, $|01\rangle$, $|10\rangle$ et $|11\rangle$ pour les qubits : q[0], q[1], q[2] et q[3].

Valeur des espérances mesurées à l'aide du simulateur de machine quantique d'IBM :

$$\langle A_1 B_1 \rangle = 0.69713$$

$$\langle A_3 B_1 \rangle = 0.70351$$

$$\langle A_1 B_3 \rangle = -0.71737$$

$$\langle A_3 B_3 \rangle = 0.710269$$

Ainsi, on peut calculer :

$$|C| = 0.69713 + 0.70351 - (-0.71737) + 0.710269 \simeq 2.82 > 2$$

On voit alors que le théorème de Bell, en particulier l'inégalité CHSH est bien violée. Ainsi les qubits n'ont pas été perturbés lors de la transmission et la source émet bien des qubits intriqués EPR. Alice et Bob peuvent alors utiliser les deux derniers qubits q[4] et q[5] pour leur clé. Puisque les qubits sont intriqués et qu'ils n'ont pas été perturbés, alors si Alice a mesuré $|1\rangle$ (respectivement $|0\rangle$), Bob aura mesuré $|1\rangle$ (respectivement $|0\rangle$).

En reproduisant les mesures sur l'ordinateur quantique à 16 qubits de Melbourne d'IBM, voici les résultats obtenus :

$$\langle A_1 B_1 \rangle = 0.42596$$

$$\langle A_3 B_1 \rangle = 0.5271$$

$$\langle A_1 B_3 \rangle = -0.39166$$

$$\langle A_3 B_3 \rangle = 0.50796$$

Ainsi, on peut calculer :

$$|C| = 0.42596 + 0.5271 - (-0.39166) + 0.50796 \simeq 1.85268 < 2$$

On voit que les résultats obtenus ne sont pas du tout ceux calculés théoriquement et mesurés grâce au simulateur. Il doit donc probablement y avoir une limite physique à la machine utilisée ici. Il se pourrait qu'un grand nombre de petites erreurs de mesure finissent par donner des résultats faux. Il serait intéressant de reprendre le circuit utilisé ici sur un autre ordinateur quantique plus performant et dont nous serions sûrs de sa capacité physique à réaliser le circuit 3.6.

3.5 Conclusion - Protocoles

Après avoir comparé les deux protocoles, on peut voir que le protocole de Arthur Ekert, E91, 3.2 apporte une subtilité que le protocole BB84 3.1 n'a pas : la possibilité que la source n'est pas corrompue grâce à la vérification de la valeur de C. En effet, nous avons vu dans la partie sur le protocole BB84 que Tim jouait le rôle de la source en émettant les qubits. Mais nous pourrions imaginer que la source puisse être extérieure à Tim et Elodie, ainsi elle pourrait être corrompue.

Chapitre 4

Conclusion

Au début de ce rapport, nous avions pour objectif de découvrir des protocoles de sécurité et de se demander s'il pourrait être envisageable de les utiliser afin d'améliorer les technologies existantes.
On voit ici que le monde quantique offre de nouvelles possibilités permettant de protéger des transferts de données. Bien que nous n'ayons aperçu que la partie théorique de deux protocoles, il semblerait qu'ils soient une solution envisageable d'amélioration des protocoles actuels comme le chiffrement RSA largement utilisé dans le commerce électronique par exemple.
Il est malgré tout essentiel de noter que la pratique et la mise en place physique de ces protocoles est compliquée et n'est probablement pas utilisable pour le moment. Malgré tout, nous pourrions imaginer, dans le futur, une mise en place de ces protocoles dans les entreprises qui échangent des données sensibles, puis progressivement chez les particuliers afin de sécuriser des transactions ou des échanges d'informations.

Bibliographie

[1] B. Zwiebach. DIRAC's BRA AND KET NOTATION. Lieu d'édition : Massachusetts Institute of Technology, 2013, 15.

[2] BUDAI Lucas, JAFFALI Hamza, NOUNOUH Ismael. Principes fondamentaux de l'information quantique. Informatique quantique. Lieu : Université de Technologie de Belfort-Montbéliard, 2014, 71.

[3] Dhoha AL-Mubayedh1, Mashael AL-Khalis2, Ghadeer AL-Azman3, Manal AL-Abdali4, Malak AlFosail, Naya Nagy. Quantum Cryptography on IBM QX. Cryptographie quantique. Lieu de soutenance : College of Computer Science and Information Technology, Cyber Security and Digital Forensics, Imam Abdulrahman bin Faisal University - Dammam - Saudi Arabia, 2019, 6.

[4] David Louapre. L'intrication quantique [en ligne]. Blog. Disponible sur : https://sciencetonnante.wordpress.com/2016/01/22/lintrication-quantique-video/ .(03/04/2020)

[5] Auteur inconnu. Évolution d'un qubit sur la sphère de Bloch [en ligne]. Blog. Disponible sur : http://stla.github.io/stlapblog/posts/EvolutionQubit.html

[6] Guy ROYER. Tenseur. [en ligne]. Lieu d'édition : Université de Nantes. http://ressources.univ-lemans.fr/AccesLibre/UM/Pedago/physique/04/maths/cadremaths.htm

[7] Guihua Zeng. A simple attacks strategy of BB84 protocol. Cryptographie quantique. Lieu de soutenance : National Key Laboratory on ISDN of XiDian University - Xi'an - China, date inconnue, 9.

[8] Pablo Arrighi, Simon Perdrix. Modèles de Calcul Quantique.

[9] Frédéric Holweck. Découverte de l'ordinateur quantique d'IBM. Lieu d'édition : Université de Technologie de Belfort-Montbéliard, 2019, 6.

[10] Artur K. Ekert. Quantum Cryptography Based on Bell's Theorem. Lieu : Merton College and Physics Department, Oxford University, UK, 1991, 3

[11] Mathematical Formalism of Quantum Mechanics. Lieu : Massachusetts Institute of Technology, 2012, 7.

[12] Michaël Monerau. Algorithmique quantique : de l'exponentiel au polynômial. Lieu : ? ? ?, 2008, 16.

[13] Jeffrey H. Shapiro. Quantum Optical Communication. Lieu : Massachusetts Institute of Technology Department of Electrical Engineering and Computer Science, 2016, 10.

[14] Aram Harrow. Quantum Computing. Lieu : Massachusetts Institute of Technology, 2016, 11.

[15] Frédéric Holweck. Introduction to Quantum Algorithms. Lieu : Université de Technologie de Belfort-Montbéliard, 47.

[16] Nikolina Ilic. The Ekert Protocol. Lieu : Department of Physics, University of Waterloo, Waterloo, ON, Canada, 2007, 4.

[17] IBM Quantum experience website. Disponible sur : https://quantum-computing.ibm.com/

Annexe A

Algorithme

Cet algorithme permet de récupérer les résultats des mesures des états des qubits mesurés avec la machine d'IBM dans la partie 3.4, dont le but est de reproduire le protocole E91 sur l'IBM QX.
Ces résultats sont ensuite formatés afin d'être utiliser pour calculer les probabilités d'obtenir $|00\rangle$, $|01\rangle$, $|10\rangle$ et $|11\rangle$ chaque fois que les bases de mesures des états des qubits de Alice et de Bob sont différentes. L'algorithme calcule ensuite les espérance des mesures : $\langle A_1 B_1 \rangle$, $\langle A_3 B_1 \rangle$, $\langle A_1 B_3 \rangle$ et $\langle A_3 B_3 \rangle$.
Language : JavaScript

```
function ComputeProbabilities(){
  let spreadSheetId = '14XDHqVDQec5nxh0lvHoMsKcgJ2aKhLYFJYATM6Tr9V0';
  let rangeName = 'resultE91!A2:B898';
  let values = Sheets.Spreadsheets.Values.get(spreadSheetId, rangeName).values;
  let d;

  //probabilities initializations
  let ket00 = [0,0,0,0];
  let ket01 = [0,0,0,0];
  let ket10 = [0,0,0,0];
  let ket11 = [0,0,0,0];

  //Esperances
  let A1B1;
  let A3B1;
  let A1B3;
  let A3B3;

  for(let i = 0; i < values.length ; i++){
    d = 0;
    values[i][1] = parseFloat(values[i][1]); //change a string proba into a number

    while (values[i][0].length < 12) {
        values[i][0] = "0" + values[i][0]; //format size of qubit state
```

```
  }

  //add probabilities every time the right values is found in the table.

  for(let index = 5; index > 1 ; index--){

    if(values[i][0][index] == 0 && values[i][0][index + 6] == 0){
      ket00[d] = ket00[d] + values[i][1];
    }
    else if(values[i][0][index] == 0 && values[i][0][index + 6] == 1){
      ket01[d] = ket01[d] + values[i][1];
    }
    else if(values[i][0][index] == 1 && values[i][0][index + 6] == 0){
      ket10[d] = ket10[d] + values[i][1];
    }
    else if(values[i][0][index] == 1 && values[i][0][index + 6] == 1){
      ket11[d] = ket11[d] + values[i][1];
    }
    else{
      Logger.log('error in ket compute')
    }
    d = d + 1;
  }

}
for(let t = 0; t<4 ; t++){ //for each array of values, format it
  ket00[t] = ket00[t]/100;
  ket01[t] = ket01[t]/100;
  ket10[t] = ket10[t]/100;
  ket11[t] = ket11[t]/100;

}
  //compute expected values
A1B1 = ket00[0] - ket01[0] - ket10[0] + ket11[0]
A3B1 = ket00[1] - ket01[1] - ket10[1] + ket11[1]
A1B3 = ket00[2] - ket01[2] - ket10[2] + ket11[2]
A3B3 = ket00[3] - ket01[3] - ket10[3] + ket11[3]


Logger.log(ket00,ket01, ket10, ket11 );
Logger.log(A1B1, A3B1, A1B3, A3B3);
}
```

Mots clefs

informatique quantique • cryptographie • BB84 • Ekert 91 • acquision de connaissances • mathématiques • qubits • Bloch • intrication quantique • IBM QX • portes quantiques • théorème de Bell • inégalité CHSH • notation de Dirac • Bra-Ket • sécurité des données

Résumé

Ce rapport reprend les bases de l'informatique quantique nécessaires à la compréhension de 2 protocoles de cryptographie quantique :
la définition d'un qubit, les postulats de l'informatique quantique, des exemples de portes quantiques, la définition de l'intrication quantique et le théorème de Bell.
Le protocole BB84 et le protocole E91 sont ensuite décrits et un exemple de chaque protocole est réalisé à l'aide d'un ordinateur quantique : l'IBM QX.
On finit ensuite par une comparaison des protocoles pour souligner la différence majeure qui donne l'avantage au protocole E91 vis à vis de la sécurité.

RAPPORT d'acquision de connaissances
rédigé au semestre de printemps 2020 par :

Alexandre DESBOS