

Veille technologique M2I 2016-2017

Les ordinateurs quantiques

Kévin ALONSO

Sommaire

Abstract	2
Définition	5
Introduction :	5
Pour qui ?	6
Pourquoi ?	7
1. L'avenir des ordinateurs quantiques	8
1.1 De nos jours	8
1.2 Les nouveautés	9
2. Les nouveaux horizons des ordinateurs quantiques	11
2.2 Vers où ?	11
2.3 La Chine progresse avec la technologie quantique	12
2.4 L'armée et les ordinateurs quantiques	14
3. Enjeux de la technologie quantique	14
3.1 Enjeux	15
3.1.1 Sécurité	16
3.1.2 Ordinateur quantique et la santé	21
3.1.3 Le monde de l'automobile	22
3.1.4 La France et le système quantique	23
4. Les dérivées de la technologie quantique	24
4.1 Le satellite quantique	24
4.2 La téléportation quantique	26
4.3 L'intrication quantique	27
Conclusion	29
Webographie	30
Définition	30
Introduction	30
1. L'avenir des ordinateurs quantiques	30
2. Les nouveaux horizons des ordinateurs quantiques	34
3. Enjeux de la technologie quantique	34
4. Les dérivées de la technologie quantique	36
Glossaire	38

Abstract

I'm Alonso Kévin, I study in IIA in Saint-Berthevin, I have a degree in computing and mobile development, now I realise master's in computing to manage project.

I chose "quantum computer to carry out my technology study because it's a really interesting subject to the future of the computing and it is a great innovation. This technology study has been done from Google Alert tools in order to create a flow of information and get all news around this subject. The report contains information of the mechanism of quantum computer, the derivatives around this technology and the impacts in the future. When I start the subject in my technology study the subject was in test but with all information that I gathered, I can see the quantum computer and all its derivatives is not a dream but reality.

The quantum computer is the last innovation from computing technology, because this machine is the only one which can execute a program two thousand times faster than supercomputers. The new technology is very important for datacenters because it can compute algorithms in a short time and to realise economic energy because the software runs shorter and consequently consumes less electric power. This point is very important because datacenter creates a lot of greenhouse gaz.

Nevertheless the quantum computer must be stabilized to temperature around the absolute zero which is minus two hundred and seventy three degrees celsius because this temperature is required to execute these operations and use the Qubits. The Qubits is the element used by this computer to generate calculation. The Qubit works differently than byte which is used by our computer. The Qubits works differently because your computer currently uses just 1 or 0. The supercomputer is the only one to work in this way by superimposing 1 and 0 : this is the mechanism used by the qubits. Now you know what a Qubit is and the temperature used by the machine so I can talk about « **dechoherence** ». This phenomenon is produced when the quantum computer heats. This is a nasty phenomenon produced by the Qubit because they are

not very stable for the moment. This technology (Qubit) is not in production, it is in development at the moment to solve the « **dechoherence** ».

Anyway many projects were born around the concept of the quantum computer such as the communication quantum, artificial intelligence and security.

The first serious point is the security, because with this kind of machine, no algorithm can resist to the attacks from this computer, because computer can break secret key. It decodes this in 1 hour while for a current computer, it should be many years, and this is very dangerous. That means that research must invent a new algorithm to protect banks, personal data... Banks for the moment are not secured enough if a quantum computer realise an attack in their system, this is a real danger for the economic system if a new super calculator is used by hacker.

Furthermore the data used by quantum computer are inviolable because if you listen to a conversation between two people (done by the attack "man in the middle") the quantum system detects and destroys the key and advertise the receiver and transmitter. If you want to extract data from conversation quantum it's impossible because you can't duplicate the message. The state has been changed and the message becomes unreadable. This is the reason why when quantum computers will be operational, all the other systems must be ready.

The second point the scientific work on quantum technology, is the communication, the traffic and the increase of the number of Qubits in the quantum computer. The communication is noticeable progress because when this technology starts you can't communicate with another system more than ten kilometre away. But now China has sent a satellite quantum which can communicate with two cities, and this progress allows to make a communication more than two thousand five hundred kilometres : it is a real evolution of this type of project. China wants to test currently this system and hope to put in place by 2030 all of their network of communication and the cost of this installation it is around twenty two million Euros (25 million dollars). This network is much secured. Furthermore with this quantum technology the country would like

to be independent because with this method China can grow up their research (military, weapons...) and this worries the other country (Example: United-State of America). This evolution it is an alternative of the use of quantum computer, and there are other projects like calculation of the traffic network and optimise it. This method has been tested in Beijing (Pekin) and the result is very good. Unfortunately the big problem to execute this calculus it is the number of Qubits : 200 Qubits should be required when the max number today in a computer is fifty Qubits : this is one of the reason why this method is still under test.

Finally the quantum computer is in development for the moment and scientists think the new super calculator arrive around two thousand thirty if the number of Qubit reaches two hundred, even though IBM is making very big progress in this field because it overtakes the Qubit record in the processor (they reached 15 stable Qubits). Through all the research and evolution (derived from the initial system) done in quantum computing it revealed elements at the beginning was not intended as teleportation which is the mode of operation of the data transmission, communication Quantum information. This discovery allows us to better understand the security mechanism and this is why information transmitted between two quantum machines is inviolable.

Finally this technology is recent and for the moment the quantum computer exists but there are not in production yet. I think this super computer will be ready in the next years (2030) because all countries start to develop their own super calculator and if one of them reach to work with this technology the others must also do it, because their security may be threatened. The quantum computer is the computer of the future, for communication, army, and data center management.

Définition

Qu'est-ce que la quantique ? Elle fonctionne d'une manière différente des machines que nous utilisons, car comme vous le savez un ordinateur utilise des bits qui sont représentées par des « 1 » ou « 0 ». Nos machines fonctionnent en manipulant ces valeurs. L'ordinateur quantique des qubits*. Ils permettent manipuler les deux états c'est-à-dire de superposés le 1 et le 0 afin d'obtenir les deux valeurs qui lui permettent d'avoir une vitesse de calcul supérieur aux autres machines.

Exemple de superposition des valeurs :

Qubits : deux valeurs à la fois



Les ordinateurs que nous utilisons actuellement codent les informations en séries de bits (0 ou 1). Un ordinateur quantique utilise des qubits, qui peuvent prendre deux valeurs à la fois (0 et 1) selon le principe de « superposition » que permettent les propriétés quantiques de la matière. Au sein du qubit, la part du 1 peut varier entre 0 % et 100 % (de gauche à droite de la première série), et de la même manière la part du zéro (de gauche à droite de la deuxième série).

Introduction :

Les ordinateurs quantiques ont un fonctionnement complètement différent des ordinateurs habituels. Nos ordinateurs que nous connaissons à l'heure d'aujourd'hui peuvent établir seulement un état « oui » ou « non », ou communément retranscrit en informatique par 0 ou 1.

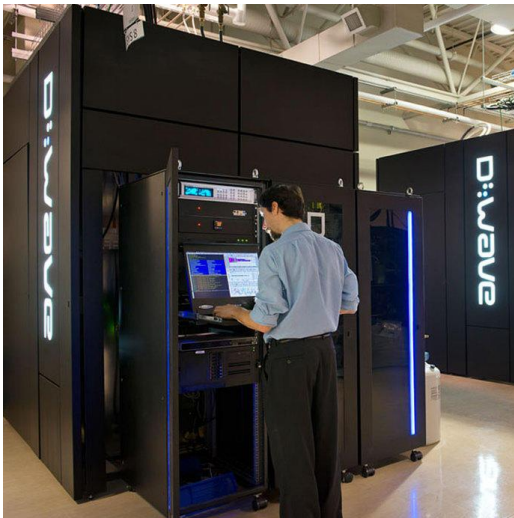
Les nouveaux ordinateurs que veulent mettre en place les entreprises ou les grands groupes comme « Google » peuvent traiter de manière différente les résultats c'est-à-dire qu'un 0 ou 1 peut être à la fois un « oui » ou un « non ».

La puissance de ces supers calculateurs montre un danger potentiel pour n'importe quel type de cryptage qui peut être déchiffré facilement, un exemple pour montrer cette super puissance : il faut un millier d'ordinateur actuel pour faire le travail d'un ordinateur quantique c'est ce que nous explique « Audrey DUFOUR » dans son article. La problématique que rencontrent ces machines est de pouvoir contenir leur puissance afin de garder un minimum de sécurité dans les réseaux actuels (logiciel, base de données...).

Pour qui ?

Les principaux acteurs qui veulent ou voudront utiliser des ordinateurs quantiques sont pour le moment des sociétés de grande envergure, comme IBM, NASA, GOOGLE, CNRS*. Seul les grandes entreprises peuvent en avoir l'utilité pour l'instant de plus leur financement de conception coûte extrêmement cher, les Américains (Google, Microsoft, Intel, IBM) ont investi des centaines de millions de dollars dans la conception de ces machines, mais également la France avec le CNRS.

De plus ces machines sont très volumineuses, sont installées uniquement dans des data center* :



Pour maintenir une telle performance de traitement il faut bien évidemment refroidir le cœur de l'ordinateur. Les températures de maintien sont impressionnantes elles atteignent les - 237 degrés Celsius ce qui est impossible à maintenir chez un particulier, car cela demanderait une trop forte consommation d'énergie.

Enfin ce type d'ordinateur est programmé pour une tâche précise avec un algorithme, il est encore très loin du principe de fonctionnement de nos ordinateurs qui nous permettent de faire de la recherche et du traitement de texte. Il reste relativement instable à cause de la décohérence lors de la superposition des « 0 » et « 1 »).

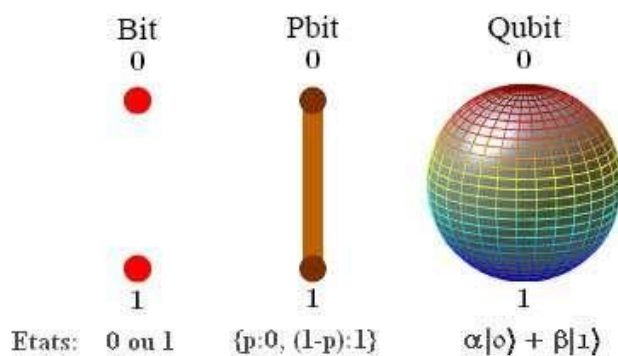
Pourquoi ?

Pourquoi utiliser des ordinateurs quantiques alors que l'informatique actuelle est déjà très performante ?

Ces performances vont permettre d'être meilleur dans la « factorisation » qui est une méthode qui est fortement utilisée pour la cryptographie des données, mais pas seulement, car ils sont également performants lors de phénomènes météorologiques (exemple les éruptions solaires). Ils permettraient également de gérer les satellites à des grandes vitesses afin de permettre d'assurer un guidage satellite pour des avions ou même la continuité du fonctionnement des objets connectés et des voitures autonomes.

Ils permettent également d'améliorer la gestion des Big Data, car il peut traiter des milliers de données à la seconde (2300 fois plus vite qu'un ordinateur ordinaire), le traitement de données réalisé par la mécanique quantique (base sur lequel ces ordinateurs sont créés) prend seulement quelques minutes contrairement à nos machines qui mettraient plusieurs années.

Ce qui leur permet d'aller extrêmement vite et leur unité utilisée qui est le qubit :



Comme le montre cet exemple, il est constitué de milliers de bits. Nos machines utilisent le Bit que l'on peut voir à gauche du schéma.

Grâce à leur forte vitesse de calcul, ces machines ont un atout économique, car elles permettent de gagner un maximum de temps sur le calcul des trajets, exemple avec la NASA qui a besoin de calculer l'itinéraire le plus court afin de réduire les dépenses d'un voyage dans l'espace, mais également améliorer fortement l'intelligence artificielle qu'il ne faut pas oublier est de plus en plus présente de nos jours.

Malheureusement ces ordinateurs restent encore à l'état de test, car ils sont encore plus ou moins instables, même s'ils sont rapides en vitesse de traitement ils peuvent également casser les chiffrements les plus complexes en un rien de temps.

1. L'avenir des ordinateurs quantiques

1.1 De nos jours

L'informatique quantique a longtemps été comme une technologie inatteignable à cause de sa complexité de mise en place et de leurs instabilités.

Google est très friand de ce genre d'innovation, car elle est dotée d'une puissance largement supérieure à nos super calculateurs que nous possédons dans nos data centers actuels.

L'ordinateur quantique fonctionne à l'aide de Qubit, c'est cette unité qui permet d'atteindre des grandes vitesses de calcul mais également de traiter une valeur que nous ne maîtrisons pas c'est-à-dire utiliser dans un algorithme la notion « **Je ne sais pas** », à l'aide de la superposition des bits comme nous avons pu le voir précédemment.

Malheureusement pour l'instant le calcul à l'aide du Qubit est instable, car ils ne peuvent pas garder en mémoire une valeur. Le Qubit n'est pas restreint par l'assimilation d'une seule valeur à la fois comme le bit, de plus cette unité est conditionnée pour ne réaliser qu'une et une seule tâche. Elle est coupée de l'environnement extérieur (ne fonctionne pas avec les autres éléments du système contrairement au bit). Microsoft a ouvert une section de recherche spécialisée dans la quantique ainsi que Google et IBM, pour le moment seuls les entreprises de grande envergure peuvent investir dans ce type de recherche, car elles sont très coûteuses, des centaines de millions de dollars (les chiffres restent pour le moment secrets).

Bien entendu si cette science n'est pas encore stable et est très onéreuse il est normal que de telles entreprises se lancent dans ce genre de projet (Google, IBM, Microsoft...), elles peuvent être un énorme avantage pour la gestion de leur data center. Pourquoi une



tel puissance dans les centres de données, car les flux de données sont en constante augmentation et les ordinateurs actuels qui permettent de gérer ce trafic ralentissent (ils ne sont pas débordés mais leur capacité de traitement viendra à faiblir dans le futur). Ces nouvelles machines peuvent traiter six cent fois plus vite l'information, ce qui permet de réduire les coûts de traitement des données dans les centres. Il leur faut beaucoup moins de temps pour arriver au résultat souhaité et il permet également d'éviter les erreurs de traitement, car il fluidifie également le trafic ce qui réduit le nombre de collision de données*.

Pour réaliser ce type de traitement Google a mis en test un ordinateur quantique dans ses locaux qui a été mis au point par la start-up D-Wave, pour l'instant cette machine n'est pas en production mais seulement en test, car la théorie de l'ordinateur quantique pour atteindre une vitesse six cent fois plus rapide n'est pas encore atteinte. Les processeurs n'ont pas atteint la capacité souhaitée. Ils ne peuvent être équipés que de 10 à 20 Qubit or le but est d'atteindre entre 100 à 300 Qubit.



Enfin, l'ordinateur quantique soulève un problème qui est la sécurité, car les super calculateurs de nos jours permettent de créer les clefs de chiffrement pour la sécurité de nos données, et c'est ce problème qui vient à inquiéter les spécialistes. Si une telle puissance était mise à disposition tout ce qui devait mettre des années à être déchiffré ou bien même à rester secret pourrait être découvert en moins de temps qu'il n'en faut, ce qui viendrait à casser tous les algorithmes de chiffrement que nous connaissons. Il faudrait alors tout reprendre afin de rendre le chiffrement égal à la puissance de ces machines afin de pouvoir faire perdurer la sécurité de certaines données.

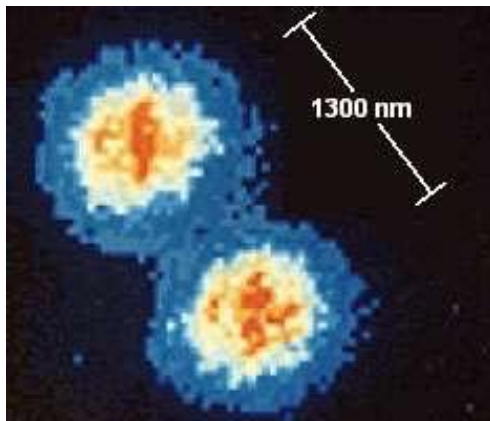
1.2 Les nouveautés

Le plus grand progrès réalisé par l'informatique reste la vitesse de calcul mais également la possibilité de faire de la superposition de données avec l'état 1 et 0 en simultané, mais pas seulement, car il peut également corriger ses erreurs à l'aide de pièges à ions* de circuits supraconducteurs*.

Les circuits supraconducteurs permettent de réaliser de l'encodage en éliminant la décohérence ce qui se passe avec les qubits et les rendent instables. Pour supprimer cette décohérence le supraconducteur se détache du bruit interférent autour de lui (c'est un peu comme si il était complètement déconnecté de tout parasite provenant de l'extérieur), ceci n'est qu'un élément permettant à la réalisation de la gestion des erreurs. Pour permettre à la machine d'isoler tous les bruits perturbateurs. Ils utilisent le diamant sur les processeurs, car il va permettre d'isoler plus facilement un bruit afin de le rendre plus visible pour l'ordinateur quantique, cette méthode va permettre de rendre stable le qubit.

Enfin, il y a le piège à ions qui va permettre de créer un qubit, pour ce faire il faut avoir deux états un état du ion stable et un état du ion en mouvement autrement dit « excité » le ion en mouvement va permettre de réaliser des qubits optiques qui vont servir de portes logiques avec une durée de vie supérieure à celle de nos ordinateurs actuels. Les qubits hyperfins* vont permettre de rendre stable le qubit tout en augmentant sa durée de vie c'est pour cela que l'ordinateur quantique utilise des piège à ions.

L'état excité des ions représente la valeur 0 et 1 du Qubit, ils sont excités ou mis au repos à l'aide d'un rayon laser qui est proche du zéro absolu en température, ici nous voyons les ions qui constitue un Qubit à l'état non excité car le rayon laser les sépare :



Malheureusement, l'ordinateur quantique n'est pas prêt d'arriver chez nous (particulier) pour le moment et ne le sera peut-être jamais. Il n'y a aucun intérêt pour le moment d'avoir une telle puissance pour faire de la simple bureautique, mais une nouveauté est apparue depuis peu en 2016 où IBM a mis en place sur son cloud la possibilité de tester à distance un ordinateur quantique pour des activités bien précises (cet ordinateur de test s'adresse essentiellement au chercheur ou au développeur informatique).

2. Les nouveaux horizons des ordinateurs quantiques

2.2 Vers où ?



Les ordinateurs quantiques vont peu à peu changer le monde de l'informatique. Les domaines de la communication vont être grandement bousculés. Les manières de transmettre un message vont changer (des satellites ou des systèmes de communication quantique) ces systèmes arrivent peu à peu. La Chine a déjà mis au point un système de communication

quantique qui permet d'augmenter la vitesse de transmission d'un message, ce qui est une révolution car actuellement nous pouvions seulement transmettre un message quantique sur une distance de 200 kilomètres hors maintenant il est possible de le faire sur 1200 kilomètres sans utiliser de répéteur (la puissance du signal est quatre fois plus puissante que ce que nous connaissons). Ce système de communication fonctionne avec une fibre car l'ordinateur quantique utilise des signaux lumineux et électrique pour transmettre une information. Cette information transite par des photons.

Le niveau d'augmentation de la distance pour transmettre un message montre également qu'une révolution sur internet est en cours, car seul des systèmes quantiques peuvent utiliser ce procédé pour le moment rien n'a été trouvé de plus puissant à ce jour. Nous parlons du « nouveau internet », mais attention qui dit nouvelle méthode de communication ou de transfert dit également sécurité modifiée, nous verrons plus loin dans le dossier le principe et les conséquences de cette nouvelle manière de sécuriser les transmissions mais également les algorithmes qui la compose.

Enfin, l'ordinateur quantique est un système beaucoup moins énergivore que nos supercalculateur qui sont actuellement en cours d'utilisation dans les grands centres de gestion de données, ce qui à l'heure d'aujourd'hui n'ai pas une donnée négligeable vue que l'écologie fait parti des priorités de chaque pays.

L'ordinateur quantique va permettre également à la médecine de progresser à grand pas dans certain domaine. Grâce à leur grande puissance de calcul pour obtenir une précision la plus optimal possible.

2.3 La Chine progresse avec la technologie quantique

Des société comme IBM et D-Wave ont réussi a construire des ordinateurs quantique, mais les scientifiques Chinois et chercheurs ont décidé de développer leur propre machine quantique qui est différente des autres sociétés. Leur machine fonctionne avec des photons multiples ce qui permet de dépasser la vitesse de calcul des supers ordinateurs mis en place. Leur architecture quantique est basé sur l'échantillonnage et l'intrication quantique de 5 photons. Cette technique change de ce que les autres chercheurs ont pus créer car leur machine est basé sur un échantillonnage à un seul photon, grâce à cette technique ils estiment être 24 000 fois plus rapide que les architectures quantique déjà créer. Les chercheurs Chinois ont fabriqué leurs propres composants pour réaliser une telle prouesse. L'exploit réalisé était qu'une théorie au début, IBM et D-Wave ce sont basés sur l'échantillonnage car c'est la base de la construction d'un ordinateur quantique, mais seul les Chinois ont réussi à utiliser un échantillonnage avec plusieurs photons. Le fait de pouvoir introduire un plus grand nombre de photons, augmente alors les traitements informatiques.

La Chine a réalisé ce projet pour pouvoir devenir autonome et améliorer son arsenal technologique. Seulement, grâce aux puces qui ont été fabriqué sur le territoire, l'ordinateur de TaihuLight est le plus puissant du monde. Il ne faut pas l'oublier mais la Chine avait déclaré en 2014 qu'elle investirait 150 milliards de dollars pour développer ses propres semi-conducteurs afin de pouvoir les inclure dans leurs ordinateurs et Smartphone qui sont fabriqués là-bas. Cette réalisation peut avoir un impact dans l'économie et les Etats-Unis craignent que le marché soit conquis par les puces Chinoise à petit prix ce qui pourrait causer du tort. Pour le moment personne ne sait si les ordinateurs quantiques vont devenir

la priorité du pays, mais de grand progrès technologique ont été effectués et cela dans un temps relativement court ce qui inquiète les États-Unis.

En effet, si la Chine possède un ordinateur quantique rapide elle pourra faire de grande prouesse dans le développement des armes du fait de la grande vitesse de calcul qui permet de prendre très rapidement des paramètres en compte et d'en éliminer d'autres pour gagner du temps. Pour le moment, il est encore à l'état de test il n'est pas encore prêt pour une mise en production l'ordinateur quantique Chinois ne peut faire que certaines tâches, or le but de cette technologie est de pouvoir réaliser n'importe quelle tâche.

La recherche des supercalculateurs quantiques est devenue obnubilante chez les chercheurs à cause de la limitation technologique que les serveurs actuels rencontrent. De plus il devient de plus en plus difficile de réduire la taille des puces. C'est une contrainte également à la baisse des coûts des ordinateurs contre une vitesse de calcul plus importante. La promesse des ordinateurs quantiques et de faire baisser les coûts, si le cas se produit alors ils prendront la place de nos serveurs actuels. Malheureusement, le problème de l'intrication joue également un mauvais rôle dans ce cas-là, car c'est à cause de ce phénomène que les ordinateurs quantiques sont inmaintenables et entraînent des instabilités des processus informatiques. Cette défaillance est comme nous l'avons vu dans la première partie due au Qubit qui est instable.

L'ordinateur quantique chinois utilise un système de photon basé sur les points quantiques (ce sont des démultiplexeurs* des atomes artificiels, des circuits photoniques* et des détecteurs). Il y a différentes façons de fabriquer un ordinateur quantique, en utilisant les qubits avec des capacités supraconductrices, c'est ce que fait l'entreprise D-Wave. À défaut du système réalisé par les Chinois, la méthode de D-Wave permet également de fabriquer simplement un supercalculateur quantique, mais qui n'est pas facile pour développer un ordinateur quantique de manière universelle. La société IBM possède déjà d'une machine quantique à 5 qubits que l'on peut même tester depuis leur Cloud.

Maintenant le fabricant cherche à réaliser un ordinateur quantique universel en utilisant toujours des qubits supraconducteurs, mais il cherche des modèles différents pour rendre le plus stable possible leur système quantique. Microsoft commence à se mettre dans la course d'un nouvel ordinateur quantique qui fonctionnera sur un calcul quantique topographique*

et avec une particule non connue qui est anyons*. La Chine est toujours dans la recherche de l'ordinateur de demain et à développé une puce neuromorphique* appelée Darwin.

2.4 L'armée et les ordinateurs quantiques

L'armée n'est pas en reste avec ce type de technologie. Elle peut leur permettre de gagner plus facilement une bataille ou d'élaborer un meilleur plan d'attaque. Ils peuvent traiter un nombre impressionnant de paramètres en un temps record. L'armée recherche ce type de système pour établir un bon plan d'attaque, le calcul de trajectoire idéale pour des drones ou la position de leurs satellites.

C'est ce que nous explique M. Pelkhanov « Autrement dit, les robots militaires du pays qui créent le premier ordinateur quantique seront en mesure de prendre des décisions plus rapidement, de travailler plus précisément, d'engager de multiples cibles, de « voir » le champ de bataille mieux et de calculer plus avant que les robots ennemis. Signifie qu'ils gagneraient des batailles, a ajouté l'observateur »

De plus le piratage de données sur son ennemi peut permettre de remporter un conflit, ce principe a été utilisé pendant la seconde guerre mondiale avec la machine Egnima. Bien entendu, en comparaison avec la puissance de décodage d'un ordinateur quantique cette ancienne machine est dépassée mais le principe reste le même, car l'outil quantique apprend par lui-même en prenant le chemin le plus court dans un algorithme.

3. Enjeux de la technologie quantique

L'enjeu principal pour le moment de l'informatique quantique est de savoir si ce développement pourra se mettre en place. Il pourra remplacer nos supercalculateurs, même si ceci est encore très puissant la venue de la quantique va permettre de faire fonctionner beaucoup plus vite les centres de données et ainsi traiter les algorithmes plus rapidement ce qui pour notre écologie est une bonne chose car un ordinateur qui traite les données consomme en moyenne 3500 kW/h hors l'ordinateur quantique ne consomme que 25 kW/h. Cet avantage de la réduction de consommation va permettre de réduire le rejet de CO2 mais également les consommations énergétiques de nos centres de données. De plus,

les enjeux vont être également le chiffrement des données à l'aide d'algorithmes encore plus puissants.

Malheureusement, il y a certaines limites qui vont venir se poser, comme les limites de la quantique c'est-à-dire de savoir si cette nouvelle façon de faire est elle stable afin de vérifier jusqu'à où nous pouvons pousser les machines dans leurs calculs, enfin il va y avoir l'aspect technique et technologique. Nous verrons tous ces points plus en détail dans les parties à venir.



Enfin, il faut trouver son but précis à l'ordinateur quantique dans son domaine car nous connaissons certaines avancées, mais une part d'inconnu persiste. La part d'inconnu pour le moment que nous n'arrivons pas à savoir est le chemin le plus court qu'à emprunté l'ordinateur pour trouver le plus rapidement possible la sortie de l'algorithme. Hors c'est ce qui intéresse les chercheurs afin de comprendre pourquoi l'ordinateur a utilisé ce chemin pour sortir de l'algorithme. C'est un enjeu majeur de connaître les raisons de ce passage mais pour le moment l'ordinateur a une mémoire qui ne va pas au delà d'une seconde c'est une des améliorations que les scientifiques aimeraient réaliser par la suite.

3.1 Enjeux

Dans cette partie nous allons voir les différents points où sont attendus les ordinateurs quantique, car leurs prouesses permettent de couvrir certain domaine. Le domaine où les supercalculateurs vont exceller est la sécurité informatique, car ils vont remettre tous nos systèmes de sécurité mais également d'algorithme à plat. La sécurité d'internet doit être renforcé avant leur arrivé, car avec la puissance de calcul des machines quantique ils n'auront pas besoin de beaucoup de temps pour déjouer nos stratégies de sécurité que nous avons mis en place. Pour ce faire les chercheurs et les mathématiciens vont mettre en place de nouveaux programmes de sécurité. Nous verrons également que les ordinateur

quantique ont une faille au niveau de la sécurité qui n'est pas des moindre, car auparavant cette technologie était dite inviolable mais des savants ont trouvé un moyen de réaliser une attaque afin de récupérer un message.

Enfin l'ordinateur quantique a un énorme enjeu qui est attendu dans le domaine de la santé où il peut faire évoluer les recherches ainsi que les traitements pour les malades. Il ne faut pas l'oublier que c'est grâce à des machines qui peuvent traiter un maximum d'informations que des traitements peuvent être élaboré ou créer. L'ordinateur quantique est utilisé également dans les « Big Data* » on parle alors de Data quantique* afin de traiter le maximum de données dans un temps records. Cette prouesse va permettre à des centres de données de réaliser le plus rapidement possible les opérations de recherche. Google a pour projet de mettre au plus vite un système quantique dans son centre de données, pour ce faire il travail avec l'entreprise D-Wave qui a réalisé la prouesse technique de mettre en marche ce type de machine. IBM c'est également lancer la course en proposant un Cloud avec un ordinateur quantique, pour le moment ce Cloud est destiné aux développeurs afin de prouver la vitesse de traitement à l'aide d'algorithme (innovation majeur, ou IBM est le seul pour le moment à avoir 5 Qubits à un état toujours stable).

Pour le moment, nous entendons essentiellement parler des Etats-Unis ou de la Chine mais la FRANCE n'est pas en reste nous commençons à tenter d'équiper nos centre de données de cette même technologie. C'est l'un des points que notre nouveau président Monsieur MACRON ne veut surtout pas négliger, afin que la France reste à la pointe de la technologie.

3.1.1 Sécurité

La sécurité est basée sur les fonctions de la cryptographie, qui permet de dissimuler un message à certains utilisateurs. De nos jours cette utilisation est indispensable avec internet afin de sécurisé les informations qui y circulent afin de garantir l'intégrité des données mais également leur authenticité.

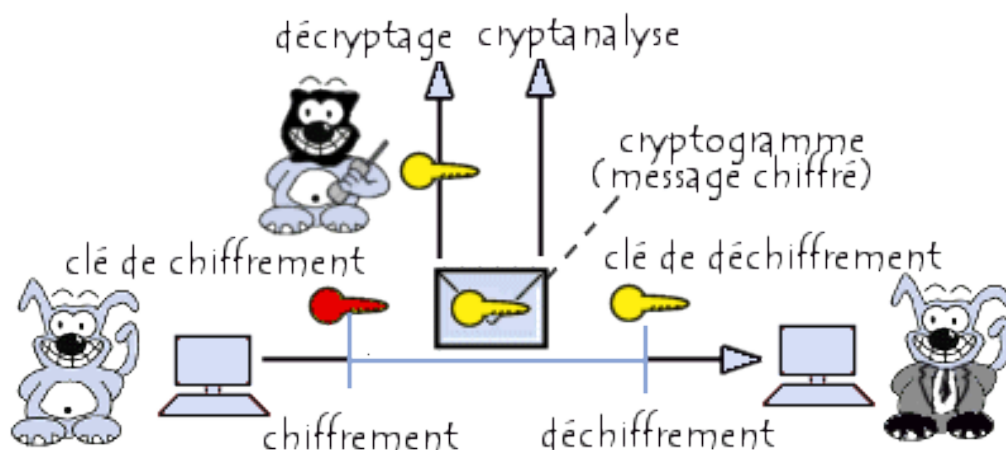
Pour reconstituer un message crypté nous utilisons la cryptanalyse, celle-ci fonctionne à l'aide d'une méthode mathématique qui se sert d'un algorithme de chiffrement, à l'aide de quatre méthodes de cryptanalyse :

- Une attaque sur texte chiffré permet de chercher la clef de chiffrement.
- Une attaque sur texte clair connu permet de retrouver une clef chiffrée à partir de texte chiffré qui connaisse le texte clair.
- Une attaque sur texte clair choisi permet de retrouver la clé de déchiffrement à partir de texte chiffré.
- Une attaque sur texte chiffré choisi permet de retrouver une clé de déchiffrement à partir de textes chiffrés

3.1.1.1 Fonctionnement de la cryptographie

Pour bien comprendre ce que l'ordinateur quantique pourra modifier dans la cryptographie nous allons faire un point sur ce qu'elle est mais également sur son fonctionnement afin de bien comprendre son procédé.

La cryptographie est une méthode de chiffrement qui va nous permettre de cacher un message lors d'une communication entre deux machines (la cryptographie n'est pas née de l'informatique elle était déjà utilisée depuis l'époque romaine). Voici un petit schéma qui représente bien ce qui se passe lors du chiffrement du message :



















Les clefs de chiffrement que nous voyons sur le schéma permettent de garder l'information transmise la plus secrète possible, pour les données vraiment sensibles les ordinateurs actuels ont bien du mal à les déchiffrer car ils sont générés par des supercalculateurs qui eux ont besoins de temps pour retrouver la clef.

3.1.1.2 Fonctionnement de la cryptographie quantique

La cryptographie quantique consiste à utiliser les propriétés de la physique quantique afin d'utiliser les protocoles de la cryptographie qui permettent d'utiliser des niveaux de sécurités qui sont prouvés (c'est-à-dire non-quantiques). Un exemple important de cryptographie quantique est la distribution quantique de clés, qui permet de distribuer une clef de chiffrement secrète entre deux utilisateurs. Cette méthode permet de garantir la sécurité de la transmission grâce aux lois de la physique quantique et de la théorie de l'information.

Cette clé secrète peut ensuite être utilisée dans un algorithme de chiffrement symétrique*, afin de chiffrer et déchiffrer des données confidentielles.

Voici à quoi ressemble un schéma de chiffrement quantique des données :

Alice émet des photons Valeur en bit :								
Bob reçoit les photons à travers un filtre								
Le photon passe? Valeur en bit :	OUI 0	NON 1	NON 1	NON 1	NON 1	OUI 0	OUI 0	OUI 0
---Canal radio--- Bob : ma mesure Alice : correct	diag oui	diag non	rect oui	rect oui	rect non	rect non	rect oui	diag non
Clé reconstituée	0	×	1	1	×	×	0	×

Pour y voir plus claire de le principe de fonctionnement du chiffrement quantique nous allons partir de l'exemple du schéma qui concerne Alice et Bob.

« Le message entre Alice et Bob est composé de 0 et 1. L'échange s'effectue sur deux canaux qui sont « le canal quantique » et un « canal radio ». Le canal quantique permet de réaliser l'échange de photons et le canal radio lui va servir aux échanges (attention ce canal n'est pas protégé). La cryptographie quantique fonctionne donc avec deux photons, mais pour que les photons puisse être lue de manière informatique il faut les faires correspondre à des 1 ou 0. Pour ce faire les photons qui sont compris entre zéro degré et quarante cinq degré sont lus

comme des 0 et les photons qui sont compris entre quatre vingt dix degré et cent trente cinq degré représentent un 1.

Pour réaliser le message chiffré Alice va émettre des photons de manière aléatoire entre zéro, quarante cinq, quatre vingt dix et cent trente cinq degré. Le second utilisateur qui est Bob va recevoir les photons de Alice de manière aléatoire lui aussi, mais pour que le récepteur puisse lire le message, il y a des filtres rectiligne qui lisent les photons qui ont la valeur zéro et un filtre diagonale qui est à quarante cinq degré, à l'aide de ces deux filtres Bob va pouvoir récupérer les 0 et 1 du message chiffré.

Bien entendu certaine valeur n'ont pas d'intérêt pour le récepteur (C'est une moyenne de un sur deux), car il a pu mesurer la polarisation rectiligne d'un photon mesuré à quarante cinq degré mais malheureusement ce photon est une valeur sans intérêt car Bob récupère un alors que l'émetteur (Alice) a envoyé un 0. Il va donc falloir éliminer ces bits qui n'ont aucun sens pour Bob. Il va indiquer à Alice par le canal radio le type de mesure (rectiligne ou diagonale) et ceci pour tous les photons, de plus Alice indique également lesquels de ces photons sont correctes.

Maintenant que la clé secrète commune est constituée, il faut vérifier que personne d'autre n'écoute le canal quantique, car ici Caroline qui écoute le canal afin de trouver la clé secrète d'Alice et Bob peut faire croire à Alice que c'est Bob qui répond en envoyant les mêmes photons que Bob. Caroline pour réussir à tromper le récepteur va tenter de remettre des photons polarisé en envoyant le même photon que Alice mais il y a une chance sur 4 que le photon transmis par le hacker soit erroné et donc que le récepteur (Bob) reçois une information fausse.

Le faite de recevoir trop de message erroné cela peut être un signe pour ce rendre compte qu'une personne est en train d'écouter la conversation. Afin de réagir vite une parti des bits de la clé (photon) son abandonné ce qui va mettre en déroute la personne qui est entre les deux interlocuteurs ».

3.1.1.3 Le cryptage quantique ya t'il une faille ?

Le cryptage quantique est censé être inviolable, car les photons sont des signaux lumineux qui sont détruits leur de la première lecture, c'est grâce à la perte de ce signal que les utilisateurs peuvent détecter une attaque appelé « man in the middle* » ou plus connu sous son terme français qui est « l'homme du milieu ».

Exemple de ce type d'attaque avec Caroline :

Alice émet des photons								
Valeur en bit :	0	0	1	1	1	0	0	1
Caroline intercepte...								
Elle lit :	1	0	1	0	0	0	0	1
et réémet :								
Bob reçoit les photons à travers un filtre								
Le photon passe?	OUI	NON	NON	NON	NON	OUI	OUI	OUI
Valeur en bit :	1	1	1	1	0	0	0	0
---Canal radio---								
Bob : ma mesure	diag oui	diag non	rect oui	rect oui	rect non	rect non	rect oui	diag non
Alice : correct								
Clé reconstituée	1	X	1	1	X	X	0	X

Puis... Bob : j'ai peur que nous ayons été espionné, sacrifions le premier bit de notre clé - j'obtiens 1

Alice : je t'avais envoyé 0, nous avons été espionnés...

Remarquons pour terminer que même non repérée, Caroline n'avait pas la bonne clé, puisque le troisième bit de la clé qu'elle obtient est 0 alors qu'Alice avait envoyé 1 !

Des scientifique ont prouvé le contraire et ont pu capter la totalité de la clef secrète que les utilisateurs se sont échangés sans être détecté entre les utilisateurs qui communiquent. La prouesse technique à pu être possible, car ils ont réussi à réinjecter un signal lumineux qu'ils ont pu lire et remettre dans le tuyau du message entre les utilisateurs. La théorie quantique rend normalement impossible cette opération, car l'écouteur (l'homme du milieu) ne sait pas comment reproduire le signal que le récepteur a envoyé au destinataire. La faille pour réaliser cette opération viens du fonctionnement d'un des composants de transmission du signal, ce composant est la photodiode à avalanche*.

Composant photodiode :



Cela se produit quand le composant capte une impulsion trop forte, celle-ci le rend aveugle pendant un court instant ce qui permet au pirate informatique faire accepter toutes les polarisations possible des photons. C'est avec ce flash que la sécurité quantique peut être mise en péril et cela permet de recréer le même type d'attaque que nous connaissons mais de manière plus évoluée. Malgré tout ce système reste l'un des plus sécurisé, c'est pour cela que nous ne devons en aucun cas négliger la création de nouveaux algorithmes qui vont permettre de résister à l'informatique quantique. Les ordinateurs pourront dans un futur proche casser nos algorithmes actuels de chiffrement du fait de leurs grandes capacités de traitement et de calcul.

3.1.2 Ordinateur quantique et la santé

La médecine commence également à s'intéresser aux ordinateurs quantique à cause de leur capacité à traiter un grand nombre de données mais surtout pour leur vitesse de calcul. Ils vont être utiles pour résoudre des problèmes très complexes. De nos jours quand on parle du futur de la santé nous sommes souvent sur le sujet de la médecine préventive, médecine sur mesure, automatisation de quelques opérations par des robots, au croisement des données des patients pour connaître au mieux le profil des patients.

On ne pense jamais à la capacité des ordinateurs et de leurs vitesses de calcul pour arriver à de tels résultats. La prochaine grande avancée est de pouvoir croiser et de lire une énorme quantité de données très rapidement. C'est à ce moment là que les ordinateurs quantiques deviennent intéressants dans le domaine de la santé. Monsieur Thom directeur des services aux professionnels de l'entreprise D-WAVE explique que l'ordinateur quantique « rendra plus facile l'analyse d'information génétique, ou de répertorier le patrimoine génétique des individus » de plus « les chercheurs pourront utiliser ces informations pour établir, des options de traitement plus facilement ». Les super calculateurs pourraient être très utiles dans le domaine de radiothérapie.



La radiothérapie est une des méthodes de soins les plus utilisés dans le traitement du cancer, car pour avoir de bon

résultat avec ce traitement il faut calculer au mieux le dosage du médicament pour minimiser les effets secondaires sur les patients.

Malheureusement pour le moment cette tâche est réalisée par un dosimétriste* qui travaille avec des logiciels pour calculer le dosage du médicament. Le logiciel ne marche pas de la meilleure des façons, il y a trop de paramètres et de variables à prendre en compte et nos machines actuelles ne peuvent pas tout traiter, car elles sont limitées en puissance.

L'ordinateur quantique n'est pas limité et peut réaliser de très lourds traitements en un temps record, pour obtenir un résultat plus précis dans les traitements. Une étude a déjà été testée au centre de recherche du cancer à Roswell Park qui est un établissement reconnu à la pointe de la radiothérapie. C'est pour cela que les super calculateurs prennent de l'importance, dans ce domaine ils permettront également de créer de nouveaux médicaments qui seront dosés au plus proche de la maladie sans avoir de mauvais effets secondaires sur les patients.

3.1.3 Le monde de l'automobile

Le groupe Volkswagen veut investir dans les ordinateurs quantiques car ils peuvent être utiles dans le domaine des véhicules autonomes, mais pas seulement il y a aussi les processus assistés par intelligence artificielle, les usines intelligentes, machine Learning et de la mobilité intelligente.

L'informatique quantique a une utilité dans la mobilité intelligente. Les ordinateurs servent à calculer des itinéraires très fréquentés par les automobilistes où les embouteillages peuvent se créer. Les super calculateurs seraient utiles dans la prévision d'un embouteillage avant que celui-ci ne se produise, c'est pour cela que ces systèmes entrent en jeu. Leur capacité de traitement pourrait traiter les milliards de variables à prendre en compte. Pour le moment les machines actuelles ne peuvent pas réaliser un tel traitement.



Actuellement la société D-WAVE est mise en test dans la ville de Pékin l'optimisation du trafic routier. Les chercheurs ont déjà développé des algorithmes pour rendre le trafic plus fluide. Bien

entendus pour que de tels algorithmes soient traités un super ordinateur est nécessaire car nos ordinateurs vont mettre environ entre trente à quarante minutes pour lire et analyser toutes les variables or la machine quantique peut réaliser la même opération en ne mettant seulement que quelques secondes. La rapidité d'exécution pour ce type de prévision n'est pas négligeable, car comme nous le disons plus haut dans le document un embouteillage peut se former avant même que les ordinateurs actuels aient traité la demande. Le trafic routier peut évoluer très rapidement.

Mais alors comment marche le test mis en place pour évaluer l'algorithme des chercheurs. Dans la ville de Pékin les données ont été remontées par dix mille taxis afin d'avoir le maximum d'informations possible sur le trafic routier, ces données ne sont pas toutes utilisées par l'algorithme, car certaines n'ont pas d'utilités pour réaliser cette opération. Une fois les données essentielles recueillies le programme va permettre de calculer le déplacement des objets. De nos jours nous commençons à voir de plus en plus de véhicules autonomes arriver sur le trafic routier et bien ces ordinateurs quantiques vont contribuer également à la bonne distribution de l'information dans un temps très réduit pour rendre les véhicules encore plus performants.

Enfin ils peuvent également contribuer aux usines de fabrication qui sont robotisées, le traitement des algorithmes peut encore optimiser le processus de fabrication. Ils prennent en compte un très grand nombre de variables pour avoir un retour sur l'analyse. Le but des ordinateurs quantiques et de ses programmes est d'apprendre par eux-mêmes, mais également de retenir la solution la mieux adaptée au problème que l'algorithme devra traiter.

3.1.4 La France et le système quantique

Notre pays n'est pas en reste sur ce type de technologie, ATOS a effectué des recherches afin de créer son propre supercalculateur. Pour le moment il est en état de teste et n'est pas totalement opérationnel, mais il est hors de question pour la France de ne pas posséder ce type de technologie dans nos centres de données, pourquoi car lors de la venue de ces nouvelles machines sur la toile il est important que nous en possédions également une du même genre afin de ne courir aucun risque de piratage sur nos systèmes.

Google au Etats-Unis espère mettre en route (en production) leur ordinateur quantique d'ici la fin de l'année 2017. C'est une course contre la montre qui se lance avant que la France puisse équiper ces centres de données sensibles pour ne pas être affaibli par les nouvelles machines qui peuvent casser certains algorithmes comme nous avons pu le voir précédemment dans le dossier (exemple également avec la Chine).

De plus ce qui oblige notre pays à investir dans la recherche et la mise en production de ces systèmes dans certains pays Chine, Russie commence également à se mettre aux ordinateurs quantiques. La France ne pense pas pour le moment mettre en place ce type de technologie d'ici la fin de l'année, ils estiment qu'il faudra plus de temps pour concrétiser le projet (on estime d'ici 2020 la mise en place du système quantique). Ce qui de toute façon n'est pas trop dérangeant, pour le moment les pays qui souhaitent utiliser les machines quantiques ou qui sont en cours de développement avec cette prouesse technologique n'en possèdent pas plus d'une à leur actif et sont pour le moment.

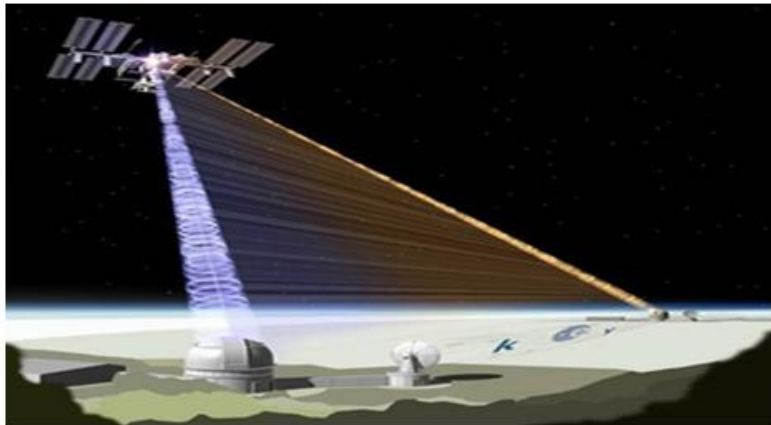
4. Les dérivées de la technologie quantique

Les dérivées de la technologie quantique nous montrent qu'il n'y a pas que les ordinateurs quantiques qui sont une innovation majeure dans le domaine des nouvelles technologies. Il y a également tous les dérivés qui peuvent en découler, car nous arrivons à parler de communication, téléportation et d'encore bien d'autres choses. Malheureusement certaines recherches restent encore inconnues ou sont en cours d'analyse pour étudier leur faisabilité dans un premier temps, puis de tenter de les mettre en phase tests.

4.1 Le satellite quantique

La Chine a lancé un satellite quantique le 16 août 2016, afin d'être les premiers à réaliser des communications quantiques pour grand public, mais également de réaliser le cryptage des conversations en les établissant sur de longues distances. Les communications sont récupérées par deux stations au sol qui sont éloignées de 2500 kilomètres. L'expérience va durer deux ans, durant ces deux années les deux stations devront être capables de transmettre des signaux mais également la clé de cryptage, sans oublier de récupérer les données du satellite.

Exemple des deux stations et de la transmission des communications :



Dispositif de communication quantique - Satellite et ses deux sites terrestres

Mais cette opération reste délicate comme nous explique Wang Jianyu « Se sera comme lancer une pièce de monnaie d'un avion volant à 100km d'altitude et espérer qu'elle vienne se ficher exactement dans la fente d'une tirelire-cochon en rotation ». Malgré tout la communication quantique est le moyen le plus fiable au niveau sécurité pour faire passer un message, comme nous le savons le chiffrement quantique est garanti inviolable du fait de sa sensibilité lors de la réception des données. La CHINE espère mettre en place d'ici 2030 toutes leurs communications sur ce système.

S'ils arrivent à réaliser cette prouesse le pays pourrais devancer les Etats-Unis et devenir un le numéro 1 des pays innovateurs dans le domaine des nouvelles technologies. Pour le moment il touche pratiquement au but, les tests avancent plus vite que prévu et une ligne commerciale quantique de communication a été mise en place entre Shanghai et Hangzhou ce qui représente une distance de 260 kilomètre entre les deux villes. La distance mise en place et encore loin de celle annoncé qui est de 2500 kilomètre, mais cela reste un réel progrès, même si cette innovation a un coût qui n'est pas des moindres car la ligne de communication s'élève à 25 millions de dollars ce qui représente 22 millions d'euros (chiffre non communiqué avec nos systèmes actuel). Le principe de fonctionnement de la ligne et de communiquer des protons afin d'empêcher toute tentative de réception de la communication par l'extérieur, comme nous l'explique le vice président de la société CCTV « Pour transmettre des informations, la ligne utilise des protons qu'il est impossible de

séparer. L'état quantique de ces protons ne peut pas être cloné. Ainsi, il est absolument impossible de mettre la ligne sur écoute ».

Le mode de communication intéresse les systèmes bancaires et gouvernementaux qui aimeraient se raccorder sur ce type de communication. Les tests doivent encore durer un an avant de pouvoir être validé.

Enfin, avec cette nouvelle façon de transmettre des informations de nouvelle recherche technologique ont pu être découverte dans le monde de l'informatique quantique.

4.2 La téléportation quantique



La téléportation quantique est une réalité proche, deux groupes de scientifique au Canada et en Chine ont effectués des recherches et des tests chacun de leur côté. ils ont obtenus des résultats identiques en transférant des données quantiques à une

distance de quelques kilomètres par une fibre optique.

Les tests démontrent la possibilité de réaliser une téléportation quantique d'informations, plus précisément sur le transfert de l'information d'un état quantique à un autre sans être interféré par la distance ou des pertes d'informations pendant le transfert. Ceci est possible grâce à l'intrication quantique qui veut qu'une particule quantique envoyée est immédiatement répercutée sur une autre. Cependant attention à ne pas confondre la téléportation quantique avec les systèmes de téléportation que nous connaissons dans les films ou livres de science-fiction. Fabio Sciarno expert en optique quantique à l'Université Sapienza, à Rome « Bien entendu, il ne s'agira pas de téléportation comme dans les films de science-fiction, mais il s'agit tout de même d'une technologie révolutionnaire », car cette communication va permettre de transmettre des informations chiffrées et impossible à décoder sauf par le récepteur. L'intérêt de ces recherches et de montrer les impacts de la sécurité au sein de l'armée, des banques, finances et de notre vie privée.

Nous pouvons utiliser le terme téléportations, car les scientifiques arrivent à détruire une particule d'un côté pour la retrouver de l'autre côté dans le même état que lors de l'envoi sans altérer le message ou la donnée.

Bien entendu pour le moment seul les photons ont été téléportés d'un endroit à un autre. Pour le moment, il est impossible de transférer un humain de cette façon, car pour ce faire il faudrait connaître tous les atomes du corps humain pour les reconstruire à l'arrivée. La téléportation du photon peut être imagée par des briques de Lego empilée que l'on transfère d'un point A à un point B voilà ce que pour le moment la téléportation quantique est capable de faire ce qui est un gros progrès pour le moment. Malheureusement le point qui pose encore problème est la distance entre les deux points.

Exemple cette structure si elle est téléportée arrivera de la même façon au point d'arrivée :



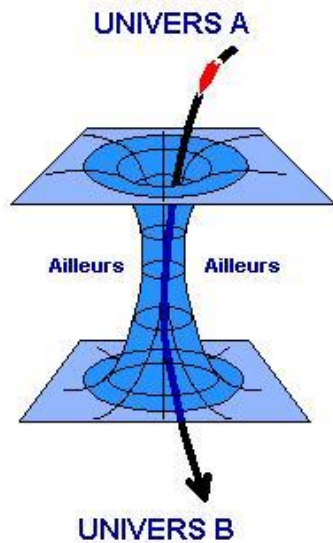
Le schéma représente bien le principe de téléportation des photons et de sa sécurité dite inviolable avec le fait que si un élément arrive changé alors celui-ci est perdu, car il ne peut pas être reconstitué. L'état du photon n'est plus le même et devient donc indéchiffrable pour le récepteur.

4.3 L'intrication quantique

L'intrication quantique joue un rôle important avec la téléportation quantique. Elle se produit lors de la communication via une fibre ou le satellite. Elle permet de lier deux photons entre eux quel que soit la distance qui les sépare. La formation de ces deux photons permet de les lier et ceux en rendant la distance comme nulle, car elle n'est pas prise en compte par ce couple d'éléments.

Ce phénomène est donc lié avec la téléportation qui utilise la communication quantique, car l'intrication va permettre aux deux photons de se délocaliser instantanément ce qui crée la téléportation.

La liaison des photons génère l'intrication quantique et également un trou de ver*.



Ce phénomène peut être comparé à un trou noir dans l'espace, car le couple de photons dans l'intrication quantique ne contient aucun lien physique. Cette découverte a également permis de comprendre plus facilement certains éléments sur le trou noir. Les scientifiques espèrent que la découverte de ces éléments dérivés de l'informatique quantique leur permettra de mieux comprendre ce phénomène.

Conclusion

Les ordinateurs quantiques ne sont plus un rêve, nous avons pu le voir tout au long de cette veille technologique. Ils remplaceront à mon avis dans un futur proche nos ordinateurs, car maintenant la vitesse et la sécurité de l'outil informatique est devenue une obligation. Attention tout de même ces machines du futur restent encore une énigme sur certains points.

Je pense que l'informatique quantique va être déterminante dans notre vie de tous les jours, au vu des recherches qu'ils permettent de réaliser, comme la médicalisation peut progresser à grand pas dans la recherche des traitements contre certaines maladies qui sont encore compliquées à traiter (le cancer). Bien entendu, d'autres innovations vont voir le jour en vue des possibilités que ces ordinateurs offrent. L'avancé dans l'armement militaire, la circulation dans les grandes villes. Les villes équipées de réseaux quantiques pourront fluidifier leur trafic et peut-être même faire baisser leur niveau de pollution.

Les communications connaîtront une amélioration importante quand la distance ne sera plus un facteur gênant pour le bon fonctionnement de la transmission des informations.

Tout de même il faudra se méfier d'une utilisation détournée de cette technologie. Les pirates informatiques tenteront sûrement d'utiliser ces appareils surpuissants pour obtenir des informations confidentielles. Les terminaux possèdent une vitesse de traitement qui dépasse largement la moyenne et sont capables de mettre un système KO si celui n'est pas préparé à ce genre de menace. Le premier pays qui arrivera à mettre au point un ordinateur quantique aura un avantage sur les autres. L'avantage sera autant économique que stratégique, car les communications seront inviolables (point négatif sachant que de nos jours nous parlons plus de cyber guerre), la possibilité de devenir autonome et ainsi de devenir le pays numéro 1 à la pointe de la technologie mondiale (exemple la Chine).

Enfin de mon point de vue l'ordinateur quantique va permettre de faire des avancées impressionnantes et très utiles pour le futur, en espérant que les chercheurs réussissent à mettre au point une machine stable. Il ne faut pas l'oublier c'est à cause de la complexité des Qubits que ces machines sont encore en phase de test même si certaines entreprises arrivent à les faire fonctionner.

Webographie

Définition

« Ordinateur quantique »

Publié sur le site futura-science.com

<http://www.futura-sciences.com/sciences/definitions/physique-ordinateur-quantique-4348/>

Introduction

« L'ordinateur quantique, un rêve prochain »

Auteur : Audrey Dufour le 16/05/2016

<http://www.la-croix.com/Sciences/Numerique/L-ordinateur-quantique-reve-prochain-2016-05-06-1200758376>

1. L'avenir des ordinateurs quantiques

« L'ordinateur quantique pour les nuls »

Auteur : KingofgeekK publié 25 novembre 2013

<http://www.kingofgeek.com/2013/11/lordinateur-quantique-pour-les-nuls/>

« Informatique quantique : l'ordinateur de demain dès 2017 ? »

Reynald Fléchaux, 9 janvier 2017

<http://www.pearltrees.com/maretto/veille-technologique/id8233236#item193959598/l639>

« L'ordinateur quantique reste à construire »

Auteur : Yann VERDO publie 06/02/16

http://www.lesechos.fr/06/02/2016/lesechos.fr/021678126130_l-ordinateur-quantique-reste-a-construire.htm

« Les ordinateurs quantiques seront bientôt là mais sommes-nous prêts à la révolution qu'ils vont entraîner ? »

Publié le 9 Septembre 2016

<http://www.atlantico.fr/decryptage/ordinateurs-quantiques-seront-bientot-mais-sommes-prets-revolution-qu-vont-entraîner-jean-gabriel-ganascia-2814151.html>

« Du laboratoire à la réalité... le long chemin de l'ordinateur quantique »

Auteur : Cécile Chevré le 2 novembre 2016

<http://quotidienne-agora.fr/laboratoire-ordinateur-quantique/>

« Les ordinateurs quantiques pourraient entrer en production dès 2017 »

Auteur : Andy R le 12/01/2017

<http://pix-geeks.com/ordinateurs-quantiques/>

« Les ordinateurs quantiques prêts à bondir hors des laboratoires dès 2017 ! »

Auteur : Ludovic Louis le 10/01/2017

<https://siecledigital.fr/2017/01/10/ordinateurs-quantiques-prets-a-bondir-laboratoires-2017/>

« L'ordinateur quantique, cent millions de fois plus rapide qu'un PC »

Publié le 16/01/2017

http://lexpansion.lexpress.fr/high-tech/l-ordinateur-quantique-cent-millions-de-fois-plus-rapide-qu-un-pc_1865030.html

« Ordinateur quantique : un nouveau record pour des puces en silicium »

Auteur : Laurent Sacco publié le 20/10/2016

<http://www.futura-sciences.com/sciences/actualites/qubit-ordinateur-quantique-nouveau-record-puces-silicium-64827/>

« IBM vous laisse tester un ordinateur quantique sur son cloud »

Auteur : Julien Bergounhox publié le 06/05/2016

<http://www.usine-digitale.fr/article/ibm-vous-laisse-tester-un-ordinateur-quantique-sur-son-cloud.N390017>

« Ordinateur quantique : nouvelle mémoire avec du diamant (MAJ) »

Auteur ; Laurent Sacco publié le 25/11/2016

<http://www.futura-sciences.com/sciences/actualites/physique-ordinateur-quantique-nouvelle-memoire-diamant-maj-11990/>

« L'ordinateur quantique de Google parvient à simuler une molécule »

Auteur : Thibault Prévost publié le 09/07/2016

<http://www.konbini.com/fr/tendances-2/ordinateur-quantique-google-molecule/>

« Côté sciences : qu'est-ce qu'un ordinateur quantique ? »

Auteur : Jean-Baptiste publié le 17/12/2012

<http://www.presse-citron.net/cote-sciences-ordinateurs-quantiques/>

« Côté sciences : qu'est-ce qu'un ordinateur quantique ? »

Publié le 01/04/2017

<http://changeonsdepoque.over-blog.org/ordinateur-dans-ere-quantique.html>

« Ordinateur quantique : IBM fait une percée sur les terres du qubit »

Auteur : Reynald Flèchaux publié le 06/05/2015

<http://www.silicon.fr/ordinateur-quantique-ibm-percee-terres-qubit-115605.html>

« Le premier ordinateur quantique programmable a été créé »

Publié par MNB le 12/08/2016

<http://paris-singularity.fr/le-premier-ordinateur-quantique-programmable-a-ete-cree/>

« Pour la première fois, un ordinateur quantique parvient à simuler une molécule ! »

Auteur : Maximilien Arengi publié le 27/07/2016

<http://sciencepost.fr/2016/07/premiere-ordinateur-quantique-parvient-a-simuler-molecule/>

« L'ordinateur quantique : tout comprendre en partant de zéro »

Auteur Viencent Rollet publié le 28/12/2016

<https://cercle.institut-pandore.com/physique-quantique/informatique-ordinateur-quantique/>

« Bientôt un Internet Quantique : qu'est-ce que c'est, et qu'est-ce que ça va changer ? »

Auteur : Timo Van Neerden publié le 16/03/2015

<https://cercle.institut-pandore.com/physique-quantique/un-reseau-internet-physique-quantique/>

« Ordinateur quantique : Rigetti ambitionne de concurrencer Google »

Publié le 02/2016

http://www.atelier.net/trends/articles/ordinateur-quantique-rigetti-ambitionne-de-concurrencer-google_440073

« Tout est quantique : comment fonctionne le principe de superposition ? »

Auteur : Jonathan Sare publié le 09/06/2016

<http://www.futura-sciences.com/sciences/videos/tout-quantique-fonctionne-principe-superposition-2641/>

« Ordinateur quantique : des progrès avec les pièges à ions »

Auteur : Laurent Sacco publié le 24/01/2016

<http://www.futura-sciences.com/sciences/actualites/physique-ordinateur-quantique-progres-pieges-ions-61279/>

2. Les nouveaux horizons des ordinateurs quantiques

« La Chine ajoute un ordinateur quantique à son arsenal HPC »

Auteur : Agam Shah publié le 05/05/2017

<http://www.lemondeinformatique.fr/actualites/lire-la-chine-ajoute-un-ordinateur-quantique-a-son-arsenal-hpc-68129.html>

« Quantum computing arms race Takes Shape as China, US, Russia Vie for Supreacy »

Publié le 11/05/2017

<https://translate.google.fr/translate?hl=fr&sl=en&u=https://sputniknews.com/military/2017/05111053523495-quantum-computing-military-applications-analysis/&prev=search>

3. Enjeux de la technologie quantique

«The Grand Challenge of Quantum Computing»

Auteur : Lawrence Krauss publié le 09/06/2016

<http://bigthink.com/in-their-own-words/the-grand-challenge-of-quantum-computing>

« Comment la France veut devenir le leader des supercalculateurs »

Publié le 13/04/2016

http://www.challenges.fr/challenges-soir/comment-la-france-veut-devenir-le-numero-1-mondial-des-supercalculateurs_29419

« L'ordinateur quantique »

Emission de radio réalisé par Mathieu Vidard le 10/11/2016

<https://www.franceinter.fr/emissions/la-tete-au-carre/la-tete-au-carre-10-novembre-2016>

« L'ordinateur quantique »

Site internet de l'entreprise D-Wave

<https://translate.google.fr/translate?hl=fr&sl=en&u=http://www.dwavesys.com/d-wave-two-system&prev=search>

« L'ordinateur quantique, un défi pour la cryptographie. »

Auteur : Yann Verdo publié le 09/12/2016

https://www.lesechos.fr/09/12/2016/lesechos.fr/0211580706903_l-ordinateur-quantique--un-defi-pour-la-cryptographie.htm

« La cryptographie quantique »

<http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/quantique>

« On se rapproche encore de l'ordinateur quantique ! »

Auteur Roman Ikonicoff publié le 23/09/2016

<https://www.science-et-vie.com/article/on-se-rapproche-encore-de-l-ordinateur-quantique-7216>

« Quand l'ordinateur quantique révolutionnera la santé »

Publié en octobre 2015

<https://atelier.bnpparibas/health/article/ordinateur-quantique-revolutionnera-sante>

« Volkswagen teste l'ordinateur quantique »

Auteur : Olivier Duquense publié le 14/03/2017

<https://www.moniteurautomobile.be/actu-auto/innovation/volkswagen-teste-l-ordinateur-quantique.html>

« Volkswagen collabore avec le canadien DWave pour tester l'informatique quantique »

Auteur : Sylvain Arnulf publié le 20/03/2017

<http://www.usine-digitale.fr/article/volkswagen-collabore-avec-le-canadien-dwave-pour-tester-l-informatique-quantique.N517319>

« Volkswagen investit dans l'informatique quantique »

Auteur : Cliff Saran publié le 22/03/2017

<http://www.lemagit.fr/actualites/450415212/Volkswagen-investit-dans-linformatique-quantique>

4. Les dérivées de la technologie quantique

« Une ligne commerciale de communication quantique inaugurée en Chine »

Publié le 11/03/2017

<https://fr.sputniknews.com/international/201703111030417619-chine-ligne-commerciale-communication-quantique/>

« Téléportation quantique : possible également via la fibre optique »

Auteur Jonathan Paino 22/09/2016

<http://trustmyscience.com/teleportation-quantique-possible-via-fibre-optique/>

« Des chercheurs ont réussi à téléporter des particules »

Publié le 20/06/2016

<http://agiteur.com/teleportation-quantique-photons/>

« Le premier satellite quantique surpasse toutes les attentes »

Publié le 20/01/2017

http://french.china.org.cn/china/txt/2017-01/20/content_40144708.htm

« À quoi va servir le satellite quantique lancé par la Chine »

Auteur Grégory Rozières publié le 05/10/2016

http://www.huffingtonpost.fr/2016/08/16/satellite-quantique-chine_n_11539416.html

« L'archipel philosophique de l'intrication quantique relativiste »

Auteur Armand Simon publié le 03/06/2017

<http://www.agoravox.fr/tribune-libre/article/l-archipel-philosophique-de-l-193655>

« Intrication quantique et téléportation »

Vidéo youtube publié le 22/01/2015

<https://www.youtube.com/watch?v=wGfAhDeNqKw>

« L'intrication quantique est-elle un trou de ver ? »

Auteur : Juan Maldacena publié le 05/2017

http://www.pourlascience.fr/ewb_pages/a/article-l-intrication-quantique-est-elle-un-trou-de-ver-38390.php

Glossaire

- **Qubits** : On nomme qubit (quantum + bit ; prononcer **kiou-bite**) l'état quantique qui représente l'unité de stockage d'information quantique. Il se compose d'une superposition de deux états de base, par convention notés $|0\rangle$ et $|1\rangle$. Un état qu-bit est constitué d'une superposition quantique linéaire de ces deux états. Une mémoire à qu-bits diffère significativement d'une mémoire classique par le fait qu'un bit ne peut prendre que les valeurs 0 et 1, et une seule à la fois. Un qubit n'a pas cette restriction.
- **CNRS** : Le Centre national de la recherche scientifique, plus connu sous le sigle CNRS, est le plus grand organisme public français de recherche scientifique. Juridiquement, c'est un établissement public à caractère scientifique et technologique (EPST) placé sous la tutelle administrative du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche.
- **Collision de données** : Lors d'une collision de données celle-ci vont être éparpillé et perdu, le receveur n'obtiendra jamais le message envoyé.
- **Ions** : Particule chargée électriquement et formée d'un atome ou d'un groupe d'atomes ayant gagné ou perdu un ou plusieurs électrons
- **Supraconducteurs** : La supraconductivité (ou supraconduction) est un phénomène caractérisé par l'absence de résistance électrique et l'expulsion du champ magnétique l'effet Meissner à l'intérieur de certains matériaux dits supraconducteurs.
- **Anyons** : En physique, un anyon est un type de particule que l'on rencontre uniquement dans les systèmes de deux dimensions.
- **Quantique topographique** : Permet de réaliser des calcul quantique pour aller d'un point A à un point B.

- **Puce neuromorphique** : permet de reproduire un réseau de neurones (comme dans le cerveau) artificiels.

- **Photoniques** : La photonique est la branche de la physique concernant l'étude et la fabrication de composants permettant la génération, la transmission, le traitement (modulation, amplification) ou la conversion de signaux optiques. Elle étudie les photons indifféremment comme onde ou comme corpuscule. Le domaine d'étude de la photonique va de l'ultraviolet proche à l'infrarouge lointain, bien que la majorité des applications de la photonique résident dans le domaine du spectre visible. Le photodétecteur se trouve à la frontière entre la photonique et l'électronique et appartient au domaine de l'optoélectronique, comme les lasers à semiconducteur. La photonique est également largement associée à l'optique intégrée. Le terme photonique est aussi utilisé dans des mots composés désignant de nouvelles sciences ou technologies utilisant la lumière : nanophotonique, biophotonique. Les composants étudiés dans le cadre de la photonique sont notamment les lasers, les diodes électroluminescentes, les fibres optiques, les modulateurs optiques, les amplificateurs optiques ou encore les cristaux photoniques

- **Big data** : Le *big data*, littéralement « grosses données », ou mégadonnées (recommandé³), parfois appelées données massives⁴, désignent des ensembles de données qui deviennent tellement volumineux qu'ils en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information.

- **Chiffrement symétrique** : Cryptographie symétrique. La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé.

- **Man in the middle** : L'attaque de l'homme du milieu (HDM) ou *man-in-the-middle attack* (MITM), parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaque « homme du milieu » est particulièrement applicable dans la méthode d'échange de clés Diffie-Hellman, quand cet échange est utilisé sans authentification. Avec authentification, Diffie-Hellman est en revanche invulnérable aux écoutes du canal, et est d'ailleurs conçu pour cela.

- **Photodiode à avalanche** : Il se distingue des autres détecteurs par l'effet avalanche qui permet de générer un gain très important (qui peut-être supérieur à 500) par rapport à une PIN standard. Ce gain permet de détecter des flux lumineux très faibles et dans certaines conditions de compter les photons.

- **Dosimétriste** : réparer et planifier les traitements par radiations ionisantes en lien avec le physicien médical et le médecin prescripteur.
Mettre en oeuvre les outils permettant le calcul des doses de rayonnements ionisants afin d'optimiser les doses reçues par le patient et de protéger les tissus sains

- **Trou de ver** : Un trou de ver forme un raccourci à travers l'espace-temps.
Qubit hyperfins : Démultiplexeurs :