

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE DE BRETAGNE

Rapport

présenté en vue d'obtenir

l'UE ENG221 « INFORMATION ET COMMUNICATION POUR L'INGENIEUR »

SPECIALITE : Informatique

par

Isabelle Delignière

Les ordinateurs quantiques

Soutenu le 31 mai 2022

JURY

PRESIDENT :	M. Yann POLLET	Professeur au CNAM Paris
MEMBRE :	M. Christophe LE CLAINCHE	Tuteur au CNAM Bretagne

Le sujet : Les médias parlent beaucoup des nouveaux ordinateurs « quantiques ». Après avoir identifié les différentes générations d'ordinateurs, vous expliquerez ce qui caractérise cette nouvelle génération d'ordinateur, puis vous présenterez une architecture ou un cas d'application en matière d'informatique quantique.

Remerciements

Je souhaite dans un premier temps remercier toute l'équipe pédagogique du CNAM pour son soutien, le partage de ses connaissances, la mise à disposition des ressources et des outils nécessaires, mais aussi pour m'avoir guidée à travers chaque étape.

Je tiens également à remercier le CNAM pour la qualité de ses enseignements et l'opportunité qui m'a été offerte de poursuivre mon parcours de formation.

Je remercie particulièrement mon tuteur, Mr Le Clainche Christophe pour le temps qu'il m'a accordé, pour ses précieux conseils et son soutien.

Je remercie Mr Blondet Florian, assistant de formation, Mme Depont Valérie, référente Ecole d'Ingénieurs Cnam et Mr Dreumont Benjamin, enseignant de l'unité ENG221 - Information et communication pour l'ingénieur pour leur accompagnement et leurs conseils avisés.

Je remercie l'association AE²CNAM, Mr Bonsignour Éric, Mr Dubois Matthieu et Mr Meunier Rémi pour leur accompagnement et leur soutien indéfectible.

Enfin, je remercie mes relecteurs, Mr Berry Julien, Mr Delignière Pierre et Mr Guillou Michel, pour le temps qu'ils m'ont accordé.

GLOSSAIRE

Cohérence : état de stabilité des qubits nécessaire pour réaliser des calculs quantiques.

Décohérer : pour des qubits, perdre la stabilité de son état, lors d'une mesure par exemple.

Distribution de clés quantiques (QKD) : méthode de communication sécurisée mettant en œuvre un protocole cryptographique impliquant des composants de la mécanique quantique.

Intrication : en physique quantique, corrélation entre deux états, qui sont donc indissolublement liés. Une action sur un état se répercute sur l'autre état. La mesure de la polarisation d'un des deux photons intriqués fixe son état de polarisation et, simultanément et instantanément, fixe celui de l'autre photon, même très éloigné.

Quantum bit ou Qubit : unité de base d'information quantique - la version quantique du bit binaire classique réalisée physiquement avec un dispositif à deux états.

Superposition : en physique quantique, capacité de prendre plusieurs états en même temps.

LISTE DES ABREVIATIONS

AES : algorithme standard de chiffrement avancé (*Advanced Encryption Standard*)

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

BB84 : algorithme de chiffrement quantique créé par Charles Bennett et Gilles Brassard en 1984

CPU : unité centrale de traitement (*Central Processing Unit*)

EDVAC : ordinateur automatique électronique à variable discrète (*Electronic Discrete Variable Automatic Computer*)

EECM : méthode des courbes elliptiques d'Edwards (*Edwards Elliptic-Curve Factorization Method*)

ENIAC : intégrateur numérique électronique et ordinateur (*Electronic Numerical Integrator and Computer*)

ETSI : l'Institut Européen des Normes de Télécommunications, ETSI (*European Telecommunications Standards Institute*)

GEECM : méthode de factorisation de courbe elliptique d'Edwards utilisant l'algorithme de Grover (*Grover Edwards Elliptic-Curve Factorization Method*)

IEEE : Institut des Ingénieurs Electriciens et Electroniciens (*Institute of Electrical and Electronics Engineers*)

MD5 : algorithme Message-Digest 5 (*Message-Digest algorithm 5*)

PKC : cryptographie à clé publique (*Public-Key Cryptography*)

QBER : taux d'erreur quantique sur les bits (*Quantum Bit Error Rate*)

QKD : distribution de clés quantiques (*Quantum Key Distribution*)

RSA : algorithme de chiffrement asymétrique Rivest-Shamir-Adleman

SHA-1 : algorithme de hachage sécurisé 1 (*Secure Hash Algorithm 1*)

SHA-2 : algorithme de hachage sécurisé 2 (*Secure Hash Algorithm 2*)

SHA-3 : algorithme de hachage sécurisé 3 (*Secure Hash Algorithm 3*)

TABLE DES FIGURES

Figure 1 : L'architecture Von Neumann - Sacha Krakowiak - 2011	8
Figure 2 : Exemple d'opérateurs analogiques - Alain Brochier, François Rechenmann - 2008	9
Figure 3 : Structure schématique d'une porte analogique - Claude Chevassu – 2022	9
Figure 4 : Les portes logiques de base - Luc De Mey - 2022	10
Figure 5 : Graphique Loi de Moore du nombre de transistors par appareil - Intel - 2005.....	11
Figure 6 : La loi de Rose pour les ordinateurs quantiques de D-Wave - Steve Jurvetson - 2021	13
Figure 7 : Image en fausses couleurs d'un processeur quantique supraconducteur à 8 qubits fabriqué à l'ETH Zurich - Antonio Acín et Al. - 2017	15
Figure 8 : Plate-forme informatique quantique - Dr. Gopala Krishna Behara - 2021.....	16
Figure 9 : Tableau récapitulatif des normes notables actuelles	18
Figure 10 : Les usages de la cryptographie - CNIL - 2016	20
Figure 11 : Algorithmes de factorisation classiques versus algorithmes quantiques - IBM - 2020	22
Figure 12 : Phases de distribution des clés quantiques - Nirbhay Kumar Chaubey, Bhavesh B. Prajapati - 2020.....	24

TABLE DES MATIERES

GLOSSAIRE	3
LISTE DES ABREVIATIONS.....	3
TABLE DES FIGURES.....	4
INTRODUCTION.....	6
1 PANORAMA DES GENERATIONS D'ORDINATEURS	7
1.1 Des calculateurs mécaniques aux ordinateurs analogiques	7
1.2 Les ordinateurs numériques.....	10
1.3 L'arrivée des ordinateurs quantiques.....	12
2 L'ORDINATEUR QUANTIQUE	15
2.1 Principes de fonctionnement	15
2.2 Architecture type	16
2.3 Les normes et standards actuels.....	18
3 CAS D'APPLICATION EN CRYPTOLOGIE	20
3.1 La cryptologie traditionnelle.....	20
3.2 Les changements en cryptanalyse	21
3.3 Les avancées en cryptographie.....	23
CONCLUSION	26
ANNEXES.....	27
REFERENCES.....	31

INTRODUCTION

Les médias parlent beaucoup des nouveaux ordinateurs « quantiques ». En effet, ces dernières années, en matière de supercalcul, l'ordinateur quantique est devenu un sujet brûlant d'actualité. Pour ne citer que quelques exemples datant du début de l'année 2022, la radio France Culture a diffusé une émission titrée « *Ordinateurs et communication quantiques : la découverte d'un matériau prometteur* »¹. Le site Web zdnet.fr a lui, mis en ligne l'article « *Google affirme que l'informatique quantique arrivera dans la décennie à venir* »². Alors que le journal Le Monde a de son côté publié l'article « *La cryptographie se prépare non sans peine à l'avènement de l'ordinateur quantique* »³. Autant d'informations qui semblent prometteuses sur l'Ordinateur de demain, est-ce vraiment le cas ? Cette étude a pour but de donner un éclairage objectif sur l'ordinateur quantique.

Ainsi, pour commencer, il est nécessaire de dresser un panorama des différentes générations d'ordinateurs. Un tableau de cette évolution sera alors réalisé, depuis les calculateurs mécaniques aux ordinateurs numériques, en passant par l'analogique, pour arriver à l'ordinateur quantique.

Par la suite, un focus sur l'ordinateur quantique sera effectué. Les principes généraux de fonctionnement et une architecture type des ordinateurs quantiques seront donc décrits. Puis les normes et standards actuels seront exposés.

Après une rapide présentation de la cryptologie traditionnelle, seront abordés les changements en cryptanalyse provoqués par l'arrivée des ordinateurs quantiques, ainsi que les prochaines avancées en cryptographie.

¹ France Culture, 2022

² Zdnet, 2022

³ Le Monde, 2022

1 PANORAMA DES GENERATIONS D'ORDINATEURS

Afin de mieux appréhender le sujet des ordinateurs quantiques, il apparaît important d'effectuer une rétrospective des différentes générations d'ordinateurs. Cet état des lieux permettra de mieux visualiser leurs évolutions et de comprendre le contexte de l'arrivée des ordinateurs quantiques.

1.1 Des calculateurs mécaniques aux ordinateurs analogiques

D'après le dictionnaire Larousse, l'ordinateur est une machine automatique de traitement de l'information, obéissant à des programmes formés par des suites d'opérations arithmétiques et logiques. Ses synonymes sont calculateur digital, calculateur numérique, computer et computeur.⁴ Le mot ordinateur apparaît pour la première fois en 1955. En effet, Jacques Perret, professeur de philologie à la Sorbonne, le propose à Emile Nouel, directeur local d'IBM, qui l'avait sollicité pour le choix du nom à donner une nouvelle machine destinée au traitement de l'information.⁵ Cette étude s'intéressera aux principaux appareils destinés à réaliser et simplifier des calculs, depuis les calculateurs mécaniques aux ordinateurs quantiques.

A ce jour, l'Abacus, apparu en Mésopotamie entre 2700 et 2300 avant notre ère, est le premier instrument mécanique connu pour réaliser des calculs. Il s'agit des bouliers, les premières machines à tabuler, qui permettent d'effectuer des additions, des soustractions et des opérations de multiplication et de division. Il est depuis utilisé un peu partout dans le monde, dans le cadre de l'apprentissage du système numérique et de l'arithmétique dans les écoles maternelles et élémentaires. Après l'Abacus, la Machine d'Anticythère ou mécanisme d'Anticythère est le plus ancien calculateur, et est parfois qualifié de premier ordinateur. Elle a été retrouvée en 1900 dans une épave près de l'île d'Anticythère et servait à prédire les phénomènes astronomiques, les saisons et les festivals. Réalisée en bronze et constituée de plus 30 engrenages imbriqués dans une petite caisse en bois, une manivelle permettait de faire tourner les engrenages. Ces derniers faisaient tourner une série de cadrans et d'anneaux pour calculer simultanément des positions par rapport au soleil, à la lune et peut-être des planètes.⁶ Ensuite, au XVII^e siècle, est inventée la Pascaline, une calculatrice mécanique considérée comme la première machine à calculer. Elle permettait de réaliser des opérations d'addition et de soustraction de nombres positifs. Cette calculatrice était composée d'engrenages, ne tournant que dans un sens, autour desquels, les chiffres de 0 à 9 étaient affichés. Sous l'influence de la gravité, un sautoir se déplaçait vers la roue suivante et permettait de transporter les chiffres.⁷

Avec ces calculateurs mécaniques, les machines sont dédiées et peu encombrantes, car spécialisées dans un type de calcul. L'architecture physique est compacte. Elles ne sont pas facilement évolutives, particulièrement en termes de puissance. Les traitements sont réalisés en série avec des algorithmes dits mécaniques. Les données sont mémorisées par un mécanisme physique tel un écran, des boules, une aiguille... ou sur un support écrit tel un parchemin, du papier... ; leur capacité de stockage est réduite voire inexistante et la confidentialité des données est assurée par la protection physique de la machine.

Puis les années 1940 vont délaisser les grandeurs physiques pour donner naissance à de nouveaux ordinateurs de type analogiques, c'est-à-dire, qui utilisent des signaux électriques pour réaliser les calculs. Notamment, en 1943, est créé le premier calculateur électronique, l'ENIAC (*Electronic Numerical Integrator and Computer*), intégrateur numérique électronique et calculateur. Celui-ci avait 17 468 tubes à vide, mesurait 2,4 mètres de haut sur 0,9 mètre

⁴ Larousse, 2022

⁵ CIGREF, 2011

⁶ Simson L. Garfinkel, Rachel H. Grunspan, 2018, pages 23-31

⁷ Georges Ifrah, 2001, pages 122-125

de profondeur sur 30,5 mètres de long et pesait plus de 30 tonnes. Il disposait d'un lecteur de cartes perforées IBM pour l'entrée et d'une carte perforée pour la sortie, mais la machine n'avait pas de mémoire pour les données ou des programmes. Les nombres en cours de calcul étaient conservés dans l'un des 20 accumulateurs de l'ordinateur, dont chacun pouvait stocker 10 chiffres décimaux et effectuer une addition ou soustraction. L'ENIAC n'a pas été programmé au sens actuel du terme, mais il utilisait un câblage et des commutateurs panneau à panneau pour la programmation. Il a été conçu pour effectuer des calculs balistiques complexes pour l'armée américaine, mais sa première utilisation officielle a en fait été d'effectuer des calculs pour le développement de la bombe à hydrogène. Toujours en 1943, le Colossus a été la première machine informatique numérique électronique, c'est-à-dire construit avec des tubes. Il a été conçu pendant la Seconde Guerre mondiale par le Royaume-Uni afin de casser les codes du haut commandement militaire allemand. En 1945, Avant même que l'ENIAC ne soit opérationnel, un ordinateur encore plus puissant, l'EDVAC (*Electronic Discrete Variable Automatic Computer*), calculateur automatique électronique à variable discrète, était créé. Il avait une banque de mémoire qui stockait à la fois le programme et les données de l'ordinateur. Une unité centrale de traitement, CPU (*Central Processing Unit*) récupérait les instructions de la mémoire et les exécutait. Le programme stocké dans la mémoire principale indiquait quand les données devaient être copiées de la mémoire dans la CPU, quand les fonctions mathématiques étaient appliquées et quand les résultats devaient être réécrits dans la mémoire principale. Aujourd'hui, cette architecture dite de Von Neumann d'après les travaux de son inventeur est largement utilisée pour décrire les ordinateurs modernes.⁸

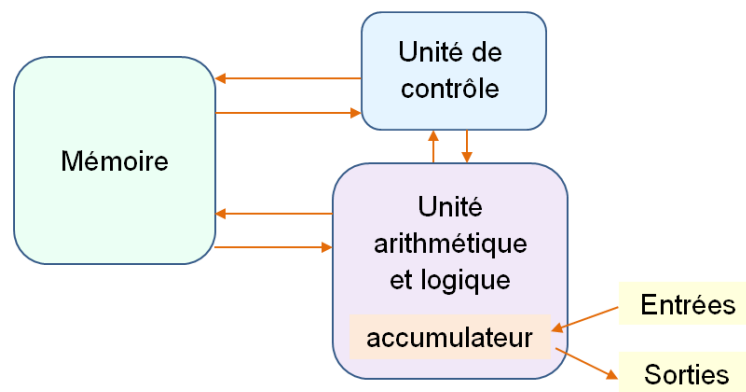


Figure 1 : L'architecture Von Neumann - Sacha Krakowiak - 2011

L'architecture dite de Von Neumann représentée en figure 1, est composée de deux unités. L'unité de contrôle qui est chargée de lire et décoder les instructions et l'unité arithmétique et logique qui s'occupe de réaliser les calculs. La mémoire permet de stocker les opérandes et les résultats des calculs en sortie de l'unité arithmétique logique. Les mécanismes d'entrée-sortie, servent à communiquer avec le monde extérieur.⁹

Ces différents ordinateurs analogiques possèdent une architecture physique centralisée, puissante mais très encombrante. Leur manque d'évolutivité est compensé en multipliant le nombre de machines pour en augmenter la puissance de calcul. Les traitements sont aussi réalisés en série avec de simples algorithmes séquentiels. Les données sont stockées soit de façon écrite, via un listing papier, ou mécanique, via des cartes perforées mécanographiques. Elles ne sont pas structurées car peu nombreuses pour cette génération d'ordinateur. Au niveau mathématique, le calculateur analogique rend possible la résolution d'un ensemble d'équations différentielles. Ceci est réalisable sans avoir à tenir compte de la nature du système dynamique réel modélisé par cet ensemble. Le circuit électrique simule donc le système. Ainsi les tensions mesurées aux bornes des composants de ce circuit sont

⁸ Simson L. Garfinkel, Rachel H. Grunspan, 2018, pages 30-31, 127-131

⁹ Sacha Krakowiak, 2011

censées évoluer comme les variables du système. Les opérations sont réalisées à l'aide d'opérateurs analogiques tels que par exemple le sommateur ou l'inverseur analogiques sur la figure 2. Avec le sommateur, la tension de sortie est la somme de toutes les tensions en entrée. Avec l'inverseur analogique, la tension de sortie est l'inverse de la tension en entrée.¹⁰

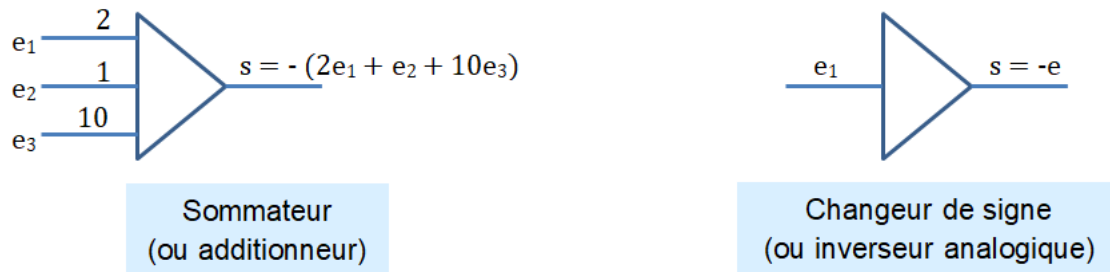


Figure 2 : Exemple d'opérateurs analogiques - Alain Brochier, François Rechenmann - 2008

Des années 1970 à 1980, les ordinateurs sont dits « hybrides », c'est-à-dire dont les signaux d'entrée sont analogiques, et les calculs et résultats sont en binaire. Le terme ordinateur signifie alors calculateur universel. Ce sont par exemple des ordinateurs électroniques dédiés au calcul scientifique et aux grandes entreprises comme le premier supercalculateur Cray-1. C'est à cette époque que l'on est passé au transistor, alors que juste avant il s'agissait des circuits électriques, des relais et des lampes. Les circuits des processeurs utilisent des portes analogiques. Les portes analogiques sont des interrupteurs électroniques capables de commuter des signaux analogiques, et commandés eux-mêmes, pour le passage de l'état ouvert à l'état fermé et inversement, par des signaux logiques. La figure 3 montre la structure schématique de chaque porte.¹¹

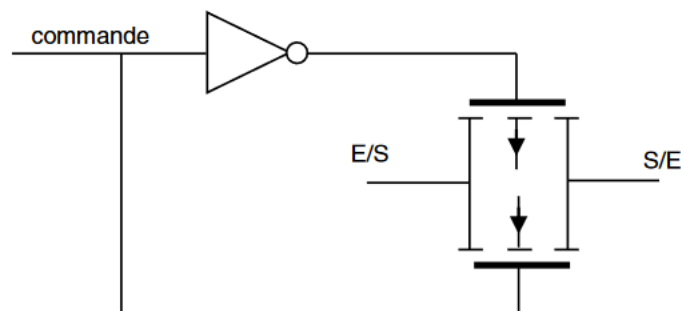


Figure 3 : Structure schématique d'une porte analogique - Claude Chevassu – 2022

Un circuit comporte quatre portes analogiques identiques. Deux transistors à effet de champ, à grille isolée par une couche d'oxyde de silicium, complémentaires, l'un à canal N et l'autre à canal P, reçoivent, sur leurs grilles, un niveau de commande nul ou positif, par rapport à la masse générale du circuit. Directement transmis à la grille du transistor à canal N, ce niveau logique traverse un inverseur avant d'attaquer celle du transistor à canal P :

- pour un niveau de commande bas (0 logique), les deux transistors sont bloqués : leurs canaux offrent, de l'entrée vers la sortie (E et S, d'ailleurs parfaitement réversibles), une résistance pratiquement infinie. L'ensemble est équivalent à un interrupteur ouvert;
- pour un niveau de commande haut (1 logique), les deux transistors conduisent et n'opposent, de l'entrée vers la sortie, que la résistance R_{ON} , de l'ordre de la centaine d'ohms. L'ensemble équivaut à un interrupteur fermé, bien qu'imparfait à cause de R_{ON} .

¹⁰ Alain Brochier, François Rechenmann, 2008

¹¹ Claude Chevassu, 2022

Ces ordinateurs centraux (*mainframe*) ont un encombrement important et leur architecture physique est aussi centralisée. Les algorithmes sont définis pour résoudre un problème particulier. Les applications sont dédiées, mais peuvent être modifiées. C'est le début des traitements réalisés en parallèle. Il est possible d'augmenter la puissance en multipliant le nombre d'ordinateurs. Depuis les années 1960, l'ordinateur va progressivement évoluer de la machine pour effectuer des calculs, à la machine pour traiter de l'information de toute nature. Les données sont stockées sur des cartes ou des rubans perforés, parfois sur les premiers disques durs qui sont plutôt réservés comme extension rapide des mémoires soit une utilisation en zones d'échange (*swapping*). C'est également le début de l'organisation des données avec les bases de données.

1.2 Les ordinateurs numériques

En 1971, Marcial Hoff de chez Intel conçoit le premier processeur monolithique commercial, un microprocesseur, l'Intel 4004. Il est réalisé sous la forme d'un seul circuit intégré. Cette technologie va progressivement se développer pour s'imposer à partir des années 90 avec les ordinateurs numériques. Les ordinateurs numériques ont des signaux d'entrée, des calculs et des résultats en binaire. En 1971 sont utilisés les premiers microprocesseurs qui par la suite ont continué à intégrer les transistors. Ce sont des circuits intégrés construits sur une puce qui permettent d'effectuer des fonctions arithmétiques, logiques et de contrôle sur cette seule puce.

En électronique numérique, les opérations logiques sont effectuées par des portes logiques. Ce sont des circuits qui combinent les signaux logiques présentés à leurs entrées sous forme de tensions. On aura par exemple 5V pour représenter l'état logique 1 et 0V pour représenter l'état 0. La figure 4 représente les portes logiques de base, la porte AND, la porte OR et la porte NOT.

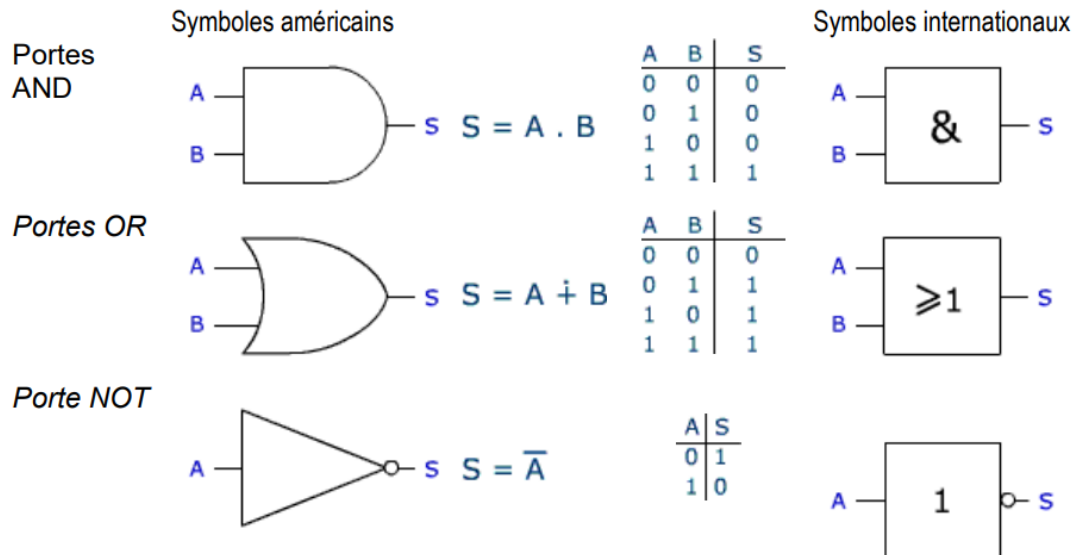


Figure 4 : Les portes logiques de base - Luc De Mey - 2022

Le nombre d'entrées des fonctions AND et OR n'est pas limité. De plus, ces trois fonctions logiques de base peuvent être combinées pour réaliser des opérations plus élaborées en interconnectant les entrées et les sorties des portes logiques. Ces combinaisons permettent d'obtenir la porte NAND : Non ET, la porte NOR : Non OU, et la porte XOR : OU Exclusif qui est en principe d'une fonction de plusieurs variables. La sortie est à 1 si la somme des entrées vaut 1, d'où son appellation « Ou exclusif ».¹²

¹² Luc De Mey, 2022

Les ordinateurs utilisant des micro-puces étaient appelés micro-ordinateurs. Ces microprocesseurs vont être largement utilisés à partir de 1976 lorsque la production de masse va en réduire le coût. En effet, en 1965, Gordon E. Moore estime que la complexité du matériel informatique va doubler tous les ans à coût constant, augmentant ainsi la puissance de calcul des ordinateurs tel que le montre la courbe de la figure 5. Il révisera cette estimation en 1975 en précisant que le doublement de complexité se fera tous les deux ans, ce qui s'est avéré exact.¹³

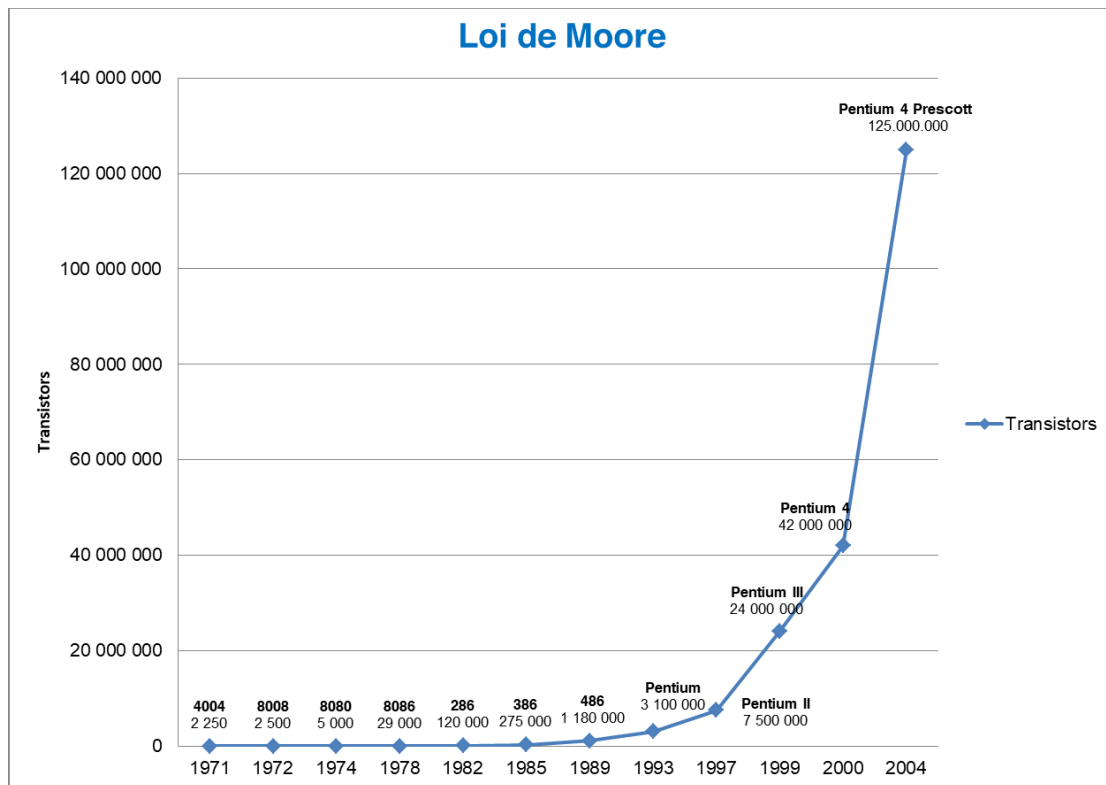


Figure 5 : Graphique Loi de Moore du nombre de transistors par appareil - Intel - 2005

A partir des années 1990, les ordinateurs deviennent de plus en plus petits et de plus en plus puissants, du fait des progrès de l'électronique et des coûts de production plus faibles. Ils sont une bonne alternative aux ordinateurs centraux, pour les entreprises où des réseaux locaux de micro-ordinateurs et des architectures de type client-serveur commencent à se développer. Plusieurs algorithmes peuvent être exécutés simultanément : c'est le début du parallélisme. Les applications sont dites universelles, se standardisent et peuvent être modifiées, parfois même par les utilisateurs. C'est également le début des systèmes d'exploitation multi-utilisateurs en réseaux, de plus en plus puissants. La puissance de traitement est augmentée grâce aux réseaux avec une flotte de machines interconnectées en réseaux.

En effet, une autre approche pour traiter plus de données plus rapidement consiste à décomposer le problème en de nombreux petits problèmes et processus en parallèle, avec une flotte de machines. Basé sur une thèse de doctorat de son cofondateur Danny Hillis à l'Institut de technologie du Massachusetts, le premier supercalculateur de la société Thinking Machines a combiné 65 536 microprocesseurs 1 bit, chacun connecté via un réseau massivement parallèle. Appelé CM-1, il s'est avéré difficile à programmer, car peu de programmeurs pouvaient visualiser des algorithmes qui s'exécutent efficacement sur des processeurs 1 bit massivement connectés. En 1991, la société a lancé le CM-5, qui utilisait 1 024 microprocesseurs 32 bits standard. La programmation était alors plus facile et avec

¹³ Gordon E. Moore, 1965

autant de processeurs, le CM-5 était l'un des ordinateurs les plus rapides qui existaient. Bien que l'idée de combiner des milliers d'ordinateurs dans une seule machine ait bien fonctionné dans les années 1990, une décennie plus tard, l'approche dominante pour résoudre les gros problèmes était l'informatique en grille (*grid-computing*), c'est-à-dire la connexion de milliers ou de millions de systèmes informatiques conventionnels via Ethernet avec des logiciels spécialisés.¹⁴ Cette technique impliquait la virtualisation des ressources informatiques pour stocker d'énormes quantités de données.

A cette période, une machine permet plusieurs types de calculs pour plusieurs centaines d'utilisateurs. Les capacités de stockage de données sont faibles et se font sur des disquettes, des bandes magnétiques et sur des disques durs. Cette dernière technique était onéreuse à l'époque. La naissance d'Internet et l'ouverture sur le monde qu'elle produit, annonce aussi le début des problèmes de sécurité informatique et des virus. En effet, la sécurité informatique n'était pas encore à l'ordre du jour.

En 2001, IBM a présenté le Power 4, le premier processeur multi-cœur au monde, une puce intégration à très grande échelle avec deux microprocesseurs 64 bits comprenant plus de 170 millions de transistors. Cette conception révolutionnaire en matière d'architecture et d'ingénierie des semi-conducteurs a permis à ces deux processeurs de fonctionner ensemble à une bande passante très élevée avec de grandes mémoires sur puce, et avec des bus et des canaux d'entrée/sortie à grande vitesse. Quatre de ces nouveaux microprocesseurs fonctionnant ensemble comme un puissant module à 8 voies ont établi une nouvelle norme industrielle et produit une vitesse d'horloge alors record de 1,3 gigahertz. La technologie d'autoréparation intégrée à la conception a catapulté les systèmes de milieu de gamme d'IBM du jour au lendemain à des niveaux de fiabilité et de disponibilité proches des ordinateurs centraux.¹⁵

En septembre 2007, lors de l'Intel Developer Forum, Gordon E. Moore, déclare que la loi Moore aura atteint ses limites d'un point de vue physique dans dix à quinze ans. En effet, la miniaturisation n'est pas infinie et ne pourra pas aller plus loin. Il faudra alors innover.¹⁶ Certains industriels travaillent donc depuis sur des microprocesseurs faits d'un empilement de transistors en trois dimensions, tandis que d'autres travaillent sur la construction d'ordinateurs quantiques.

1.3 L'arrivée des ordinateurs quantiques

Le modèle de Von Neumann a fait ses preuves, effectivement, l'intégration des composants a atteint ses limites et le temps d'accès aux données est trop coûteux. Les gains en puissance sont alors recherchés sur d'autres modèles d'ordinateur. L'idée de la création d'un ordinateur quantique prend source dans la mécanique quantique. La mécanique quantique est une théorie fondamentale en physique qui fournit une description des propriétés physiques de la nature à l'échelle des atomes et des particules subatomiques. C'est le fondement de toute la physique quantique, y compris la chimie quantique, la théorie quantique des champs, la technologie quantique et la science de l'information quantique.

La théorie des quanta a été amorcée par Max Planck, puis, sera développée principalement par Albert Einstein, Niels Bohr, Arnold Sommerfeld, Hendrik Anthony Kramers, Werner Heisenberg, Wolfgang Pauli et Louis de Broglie entre 1905 et 1924. Paul Dirac, un des pères de la mécanique quantique, a ensuite apporté des contributions fondamentales au développement précoce de la mécanique quantique et de l'électrodynamique quantique. Dirac a partagé le prix Nobel de physique de 1933 avec Erwin Schrödinger pour la découverte de nouvelles formes productives de théorie atomique. Erwin Schrödinger a par la suite conçu une expérience de pensée, afin de mettre en évidence la nature contre-intuitive

¹⁴ Simson L. Garfinkel, Rachel H. Grunspan, 2018, pages 540-541

¹⁵ IBM, 2022

¹⁶ Jon Fortt, 2007

des superpositions quantiques, dans lesquelles un système quantique tel qu'un atome ou un photon peut exister comme une combinaison de plusieurs états correspondant à différents résultats possibles. Cette expérience de pensée est connue sous le nom de la théorie du chat de Schrödinger (voir Annexe A). Enfin, Richard Feynman a reformulé entièrement la mécanique quantique, dans les années 1980 et proposé d'exploiter la physique quantique pour construire un type d'ordinateur plus puissant. Cet ordinateur est donc basé sur la logique quantique, c'est-à-dire qu'il traite l'information et effectue des opérations logiques en accord avec les lois de la mécanique quantique.

Le quantum bits ou qubit est l'unité de mesure de l'information en informatique quantique. Une façon de mesurer un ordinateur quantique consiste à compter le nombre de qubits qu'il peut traiter à la fois. En 2001, une équipe de scientifiques du centre de recherche Almaden d'IBM dirigé par Isaac Chuang a réussi à factoriser le nombre 15, ce qui donne le facteur 3 et 5, avec un ordinateur quantique qui avait 7 qubits. Bien que factoriser le nombre 15 puisse ne pas sembler être un gros problème, les chercheurs d'IBM ont alors prouvé que les ordinateurs quantiques ne sont pas seulement théoriques, mais fonctionnent réellement. À présent la course était lancée pour fabriquer un ordinateur quantique assez grand pour calculer quelque chose qui ne pourrait pas être calculé sur une machine conventionnelle. Dès lors, de nombreuses entreprises dans le monde, telles que IBM, Intel, Microsoft ou encore D-Wave, se sont lancées dans cette course.¹⁷

La loi de Rose, issue de D-Wave, suggère que les qubits d'informatique quantique devraient doubler tous les ans. Comme la loi de Moore, sur la figure 6, la ligne droite de la loi de Rose décrit une exponentielle. Mais contrairement à la loi de Moore, la puissance de calcul de l'ordinateur quantique devrait également croître de façon exponentielle avec le nombre de qubits et leur intrication. Cela est donc comme la loi de Moore mais composée.

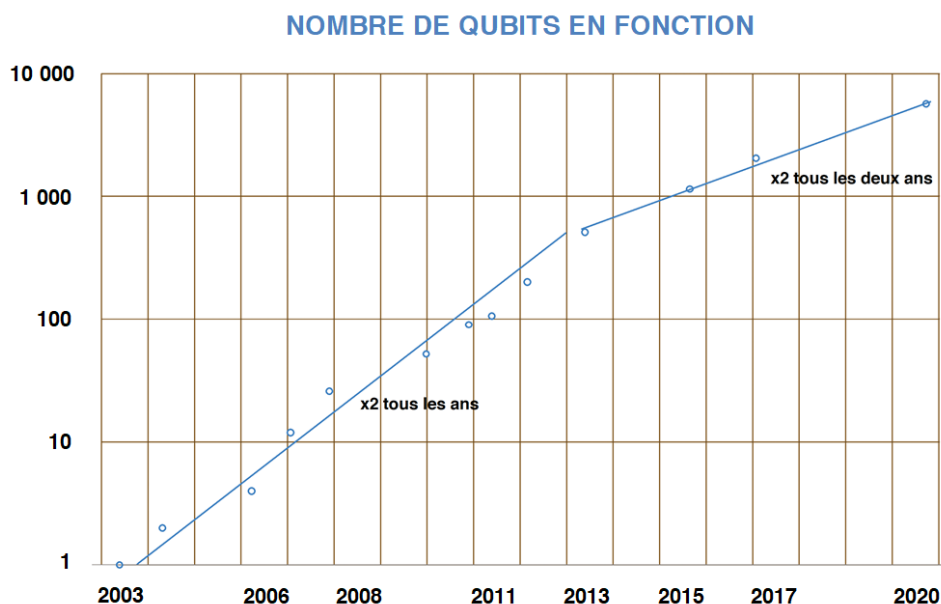


Figure 6 : La loi de Rose pour les ordinateurs quantiques de D-Wave - Steve Jurvetson - 2021

En comparant la courbe réelle du nombre de qubits en fonction par rapport à la loi de Rose, celle-ci s'est bien réalisée depuis 2003, le nombre de qubits a effectivement doublé tous les ans. Après un léger ralentissement du rythme en 2013, le retard semble être rattrapé en 2020. Les ordinateurs quantiques sont donc passés de quelques qubits dans les années 2000 à des milliers de qubits aujourd'hui selon les fabricants et types d'architecture.

¹⁷ Simson L. Garfinkel, Rachel H. Grunspan, 2018, pages 687-688

Actuellement, les traitements des données sont effectués en analogique par les ordinateurs quantiques, mais les résultats ne sont pas interprétables tels quels. Il est pour l'instant nécessaire de passer par des algorithmes via un ordinateur numérique. Les principes généraux de fonctionnement et l'architecture type seront exposés dans la partie suivante de cette étude.

Ce panorama des différentes générations d'ordinateurs montre que simplifier la réalisation de calculs complexes a toujours été d'une grande importance pour l'homme. Les techniques et technologies ont évolué en connaissant une forte accélération à partir des années 70. Les ordinateurs sont à même de résoudre des problèmes de plus en plus complexes en des temps de plus en plus courts. Ainsi, une nouvelle ère pour les ordinateurs s'ouvre avec le développement des ordinateurs quantiques et leurs promesses de puissance de calcul exponentielle.

2 L'ORDINATEUR QUANTIQUE

2.1 Principes de fonctionnement

Dans un ordinateur classique numérique, les bits d'information peuvent prendre deux états 0 ou 1. Tandis que dans un ordinateur quantique, ce sont des bits quantiques ou qubits qui sont utilisés et ceux-ci ont une infinité d'états possibles. Les qubits ont la faculté d'être dans des états de superposition de 0 et 1 et également être intriqués ensemble. La superposition, peut être expliquée sur un qubit avec l'image commune selon laquelle un qubit est à la fois zéro et un en même temps. Pour expliquer l'intrication, les mathématiques sont nécessaires, avec la notion de produit tensoriel. L'intrication qu'Einstein appelait l'action fantasmagorique à distance, combine étroitement deux qubits afin qu'ils n'agissent plus indépendamment mais collectivement. Avec la superposition, l'intrication donne lieu aux très grands espaces dans lesquels les calculs quantiques peuvent fonctionner (voir Annexe B).

Les opérations sur les qubits sont ensuite réalisées par les portes quantiques. Ces portes quantiques peuvent tirer parti des aspects clés de la mécanique quantique qui sont totalement hors de portée des portes classiques : la superposition, l'intrication et le parallélisme. Alors que les portes des ordinateurs classiques fonctionnent selon des tables de vérité, Vrai/Faux, et que la plupart des portes fonctionnent vers l'avant, les portes quantiques utilisent les transformations selon les matrices unitaires et les portes sont réversibles. Un qubit est égal à deux bits. Par exemple, un registre informatique de 4 qubits peut contenir 16 nombres différents simultanément.

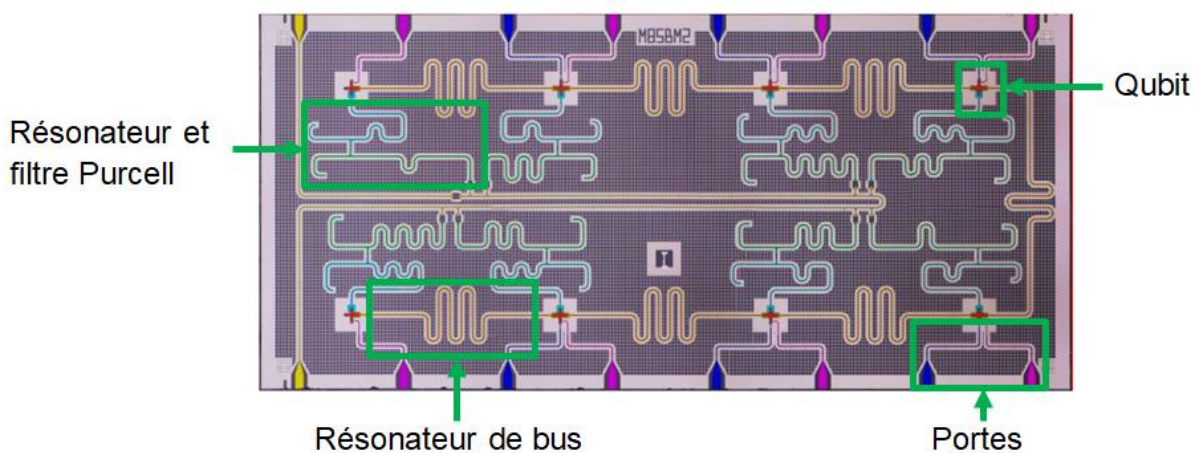


Figure 7 : Image en fausses couleurs d'un processeur quantique supraconducteur à 8 qubits fabriqué à l'ETH Zurich - Antonio Acín et Al. - 2017

Sur la figure 7, les qubits, en rouge, sont mesurés à l'aide d'une ligne de lecture commune, en jaune, en couplant chaque qubit à une paire de lecture résonateur en cyan et filtre Purcell en vert. Le contrôle Qubit est activé par des lignes de charge individuelles en violet et des lignes de flux en bleu. Les portes en bleu et en violet permettent d'agir sur les qubits. Ces deux portes sont des portes universelles permettant par combinaison de recréer les autres portes quantiques nécessaires à l'exécution des algorithmes. Le couplage entre les qubits voisins les plus proches est assuré par des résonateurs de bus en orange et sert à contrôler leur intrication.¹⁸

L'intérêt de fonctionner avec des qubits plutôt que des bits est de permettre de réaliser des calculs combinatoires complexes dans une sorte de parallélisme massif en temps réel qui prendraient trop de temps ou trop de mémoire avec un ordinateur classique ou un supercalculateur. Effectivement, la factorisation des grands nombres est un bon exemple de

¹⁸ Antonio Acín et Al., 2017

calcul pour illustrer l'utilité d'un ordinateur quantique. Celui-ci n'est pas réalisable dans un temps raisonnable avec les systèmes actuels et c'est sur ce postulat que repose le chiffrement RSA, un algorithme de cryptographie asymétrique. Néanmoins, en 1994, le mathématicien Peter Shor a développé un algorithme quantique, capable de trouver efficacement les facteurs premiers de grands nombres. Cet algorithme serait exponentiellement plus efficace qu'un algorithme classique. Un ordinateur quantique permettrait donc de grandes avancées dans des domaines nécessitant des calculs combinatoires complexes. Par exemple, pour n'en citer que quelques-uns, en chimie, il donnerait la possibilité de développer plus vite des molécules thérapeutiques ou bien en météorologie, il aiderait à améliorer les prévisions en gagnant en précision.

La suprématie quantique, c'est-à-dire le moment où les ordinateurs quantiques seront capables de réaliser des calculs hors d'atteinte des ordinateurs classiques et supercalculateurs, n'est pas encore atteinte. Les ordinateurs quantiques sont encore en phase de développement et les fabricants dans une course à l'augmentation du nombre de qubits qu'il est possible de garder cohérents dans leurs systèmes. La cohérence correspond au temps pendant lequel les qubits restent en état de superposition. Il existe actuellement plusieurs techniques pour construire un ordinateur quantique et produire des qubits. En effet, une vingtaine de méthodes sont explorées dont quatre d'entre elles sont plus particulièrement investies ; la méthode des ions piégés, les boîtes quantiques en silicium, des supraconducteurs et les ordinateurs quantiques optiques avec les états photoniques. Ces méthodes sont complexes, c'est pourquoi, dans un but de simplification, une architecture type sera présentée dans la partie suivante.

2.2 Architecture type

Il n'est pour l'instant pas possible d'interpréter directement les résultats produits par un ordinateur quantique ni d'en stocker les données. La solution actuelle est d'interconnecter l'ordinateur quantique à un ordinateur classique numérique faisant office d'interface ou de passerelle. La plate-forme informatique quantique se compose donc de deux couches, à savoir la couche informatique classique et la couche informatique quantique, qui sont représentées dans le schéma de la figure 8.

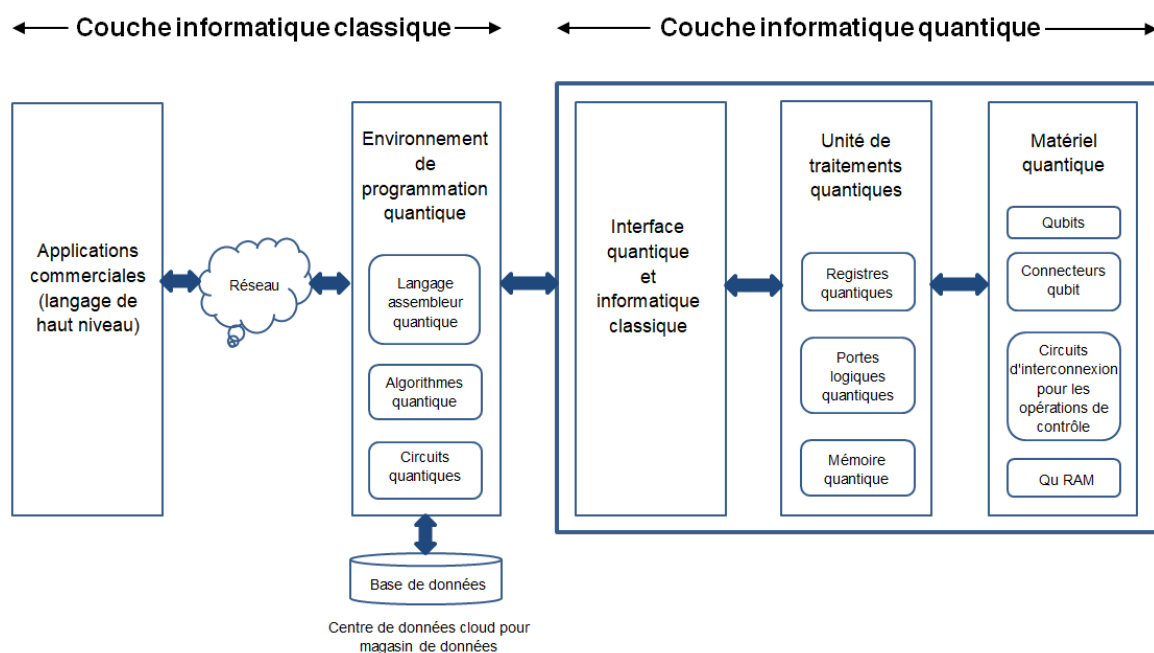


Figure 8 : Plate-forme informatique quantique - Dr. Gopala Krishna Behara - 2021

La couche informatique quantique comprend le matériel quantique, l'unité de traitement quantique et l'interface quantique-classique. Le matériel quantique couvre les qubits qui sont entourés de boucles supraconductrices pour la réalisation physique des qubits. Il se compose également de circuits d'interconnexion pour les opérations de contrôle de qubit. L'unité de traitement quantique se compose de registres quantiques, de portes logiques quantiques et d'une mémoire quantique.

L'interface quantique-classique comprend du matériel et des logiciels qui assurent l'interfaçage entre les ordinateurs classiques et une unité de traitement quantique.

La couche informatique classique comprend un environnement de programmation quantique, l'informatique en nuage (*cloud*) et des applications métier. L'environnement de programmation quantique composé de langage d'assemblage quantique pour instruire l'unité de traitement quantique, de programmes quantiques dans des langages de programmation de haut niveau, d'algorithmes quantiques pour résoudre une variété de problèmes informatiques beaucoup plus rapidement qu'un ordinateur classique et de circuits quantiques, les modèles communs pour représenter le calcul quantique. Dans ce modèle, les étapes d'un algorithme quantique peuvent être exprimées sous la forme d'une séquence de portes logiques quantiques. Chaque porte logique quantique transforme les qubits d'entrée d'une manière bien définie. En général, elle est exprimée sous forme d'opérations sur des matrices et des vecteurs d'interface de programmation d'application de haut niveau ou instructions utilisées pour composer les programmes quantiques. Les programmes quantiques impliquent principalement les tâches de mappage des entrées et sorties de la représentation classique des bits aux qubits, d'initialisation de l'état des qubits, du circuit quantique utilisant des portes logiques quantiques appropriées. Ces portes logiques permettent d'exprimer les étapes d'un algorithme quantique afin d'obtenir une mesure fiable des résultats et de mesurer l'état des qubits de sortie et le transférer sur le bit classique. L'informatique en nuage est utilisée pour stocker les données de traitement en fonction de la sortie de l'algorithme quantique. Les applications métier tirent parti des applications logicielles quantiques pour aider à répondre aux besoins métier d'une entreprise.¹⁹

Aujourd'hui, les ordinateurs quantiques sont construits sur une programmation de bas niveau basée sur des portes logiques quantiques pour gérer les étapes de calcul à exécuter dans l'unité de traitement quantique. Selon IBM, il existe cinq types d'opérations unitaires et quantiques possibles ; les portes classiques, les portes de phase, les opérateurs et modificateurs non unitaires, la porte d'Hadamard et les portes quantiques (voir Annexe C).

La complexité de l'informatique quantique implique une collaboration multidisciplinaire, engageant un grand nombre de domaines, dont notamment la physique, les mathématiques, l'informatique, la chimie, la biologie. En effet, selon IBM, chaque composante quantique requiert des compétences différentes. Ainsi, pour les services techniques, une expertise technologique générale est requise. Pour les applications, il faut connaître l'architecture et le développement d'applications. Pour utiliser des bibliothèques spécifiques à chaque cas, des connaissances de l'industrie ou du domaine sont nécessaires. Pour les bibliothèques de performances, il faut être capable de créer des algorithmes de système informatique quantique. Pour les compilateurs, les optimiseurs et les simulateurs, des compétences en mathématiques avancées et une expertise en informatique quantique sont primordiales. Pour le langage d'assemblage et les pilotes, la physique quantique et une expertise en informatique quantique sont indispensables. Enfin, pour la partie matérielle informatique quantique, les domaines de la physique quantique, la chimie et l'ingénierie sont incontournables.²⁰

L'informatique quantique est donc très coûteuse et par conséquent, c'est une forme de retour aux ordinateurs centraux dits « propriétaires » des années 60 à 80.

¹⁹ Dr. Gopala Krishna Behara, 2021

²⁰ IBM, 2021

2.3 Les normes et standards actuels

Les spécifications techniques des différentes plates-formes informatiques quantiques sont de nature hétérogène, à la fois au niveau des logiciels et du matériel impliqué dans l'unité de traitement quantique. Elles sont déterminées par les différents constructeurs encore en phase de recherche et développement tels que D-wave, Google, IBM, Microsoft, etc.

Les normes sont des documents publiés qui établissent des spécifications techniques et des procédures conçues pour maximiser la fiabilité des matériaux, produits, méthodes ou services que les gens utilisent au quotidien. Les normes technologiques peuvent également fournir un cadre qui permet aux appareils de différents fabricants de communiquer entre eux. Dans le processus, les normes fournissent une base stable mais en constante évolution qui permet à des industries entières de se développer et de prospérer. Ainsi, peuvent être considérées comme des procédés. En les appliquant, les fabricants obtiennent des informations très détaillées sur la façon dont les appareils s'identifient, comment les données circulent entre eux et comment elles sont sécurisées, pour ne citer que quelques exemples.

Pourquoi les normes sont-elles importantes ? Les normes constituent les éléments de base du développement de produits en établissant des protocoles cohérents qui peuvent être universellement compris et adoptés. Cela contribue à la compatibilité et à l'interopérabilité, simplifie le développement de produits et accélère la mise sur le marché. Les normes facilitent également la compréhension et la comparaison des produits concurrents. Étant donné que les normes sont adoptées et appliquées à l'échelle mondiale sur de nombreux marchés, elles alimentent également le commerce international. Enfin, la standardisation permettrait d'assurer l'interopérabilité des systèmes de différents fabricants, l'intégration dans les réseaux de télécommunications conventionnels, de stimuler le développement d'applications sur des interfaces communes, de stimuler une chaîne d'approvisionnement en composants pour les technologies quantiques et une garantie de sécurité. L'informatique quantique est encore en cours de recherches et développement, avec de nouvelles méthodes de calculs quantiques qui émergent fréquemment. C'est pourquoi elle a besoin d'une liberté totale pour innover et grandir.

Néanmoins, quelques normes ont commencé à émerger, le tableau de la figure 9 récapitule ces normes notables.

Identifiant	Objet	Date d'émission	Portée
IEEE P1913	Communication quantique définie par logiciel	03/2016	Norme Internationale
ETSI GS QKD 011 V1.1.1	Distribution de clé quantique; caractérisation des composants : caractérisation des composants optiques pour les systèmes de distribution de clés quantiques	05/2016	Spécification de groupe Européenne
IEEE P2995	Conception et le développement d'un algorithme quantique	06/2021	Norme d'essai Internationale
IEEE P7130	Définitions d'informatique quantique	09/2021	Norme Internationale
IEEE P7131	Mesures de performance et analyse comparative des performances de l'informatique quantique	09/2021	Norme Internationale
IEEE P3120	Architecture informatique quantique	11/2021	Norme Internationale
IEEE P3155	Simulateur quantique programmable	02/2022	Norme Internationale

Figure 9 : Tableau récapitulatif des normes notables actuelles

En effet, l'Institut des Ingénieurs Electriciens et Electronicien, IEEE, (*Institute of Electrical and Electronics Engineers*) qui est une association professionnelle internationale, a émis plusieurs documents de standardisations sur lesquels elle travaillait depuis 2017. A commencer par le document IEEE P7130, norme pour les définitions d'informatique quantique, dont le but est de fournir une nomenclature générale pour l'informatique quantique. Cette norme peut être utilisée pour normaliser la communication avec les projets matériels et logiciels connexes. Elle a également fait paraître les documents IEEE P7131, norme pour les mesures de performance et l'analyse comparative des performances de l'informatique quantique, IEEE P1913, norme de communication quantique définie par logiciel, IEEE P2995, norme d'utilisation d'essai pour la conception et le développement d'un algorithme quantique, IEEE P3120, norme pour l'architecture informatique quantique et IEEE P3155, norme pour simulateur quantique programmable.²¹

De son côté, l'Institut Européen des Normes de Télécommunications, ETSI (*European Telecommunications Standards Institute*) a publié, en 2016, sa première spécification concernant les ordinateurs quantiques. Le document ETSI GS QKD 011 V1.1.1 spécifie les paramètres de performance et quinze procédures pour un étalonnage traçable des composants de la couche quantique dans la distribution de clé quantique. Effectivement, les procédures définies pour l'étalonnage du matériel de distribution de clé quantique sont essentielles pour assurer la sécurité et fourniture de la chaîne d'approvisionnement. L'ETSI a depuis sorti d'autres documentations dont nombreuses d'entre-elles portent sur la cryptographie. Si la majorité de ses publications sont sur la distribution de clé quantique, elle s'intéresse aussi à l'ensemble de la sécurité informatique face au quantique. Ainsi, elle a notamment publié un guide sur l'impact de l'informatique quantique sur la sécurité des systèmes technologies de l'information et de la communication. Elle donne dans celui-ci des recommandations sur la continuité des activités et sur la sélection d'algorithmes.²²

En effet, les ordinateurs quantiques pourraient bouleverser le paysage actuel de la cryptologie. L'informatique quantique, bien que récente, possède donc déjà quelques normes à son actif.

²¹ Institut des Ingénieurs Electriciens et Electronicien (IEEE), 2022

²² Institut Européen des Normes de Télécommunications (ETSI), 2022

3 CAS D'APPLICATION EN CRYPTOLOGIE

3.1 La cryptologie traditionnelle

D'après le dictionnaire Larousse, la cryptologie est la science des écritures secrètes, des documents chiffrés, c'est-à-dire du chiffrement. Elle réunit donc la cryptanalyse et la cryptographie. En effet, d'un côté, la cryptographie est l'ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données. De l'autre côté, la cryptanalyse est l'ensemble des techniques mises en œuvre pour tenter de déchiffrer un message codé dont on ne connaît pas la clé.²³

Historiquement, la Scytale, également connue sous le nom de bâton de Plutarque, est l'outil le plus ancien connu pour chiffrer et déchiffrer un message. Elle était utilisée dans un but militaire par les Spartiates en 404 avant notre ère. Il s'agissait alors d'un chiffrement par transposition à l'aide d'un bâton et d'une lanière de cuir. Des lettres étaient ainsi interverties pour former les mots comme pour les anagrammes. Plus proche de notre époque, la cryptologie a été largement utilisée lors de la Seconde Guerre mondiale avec Enigma par les allemands et la machine de Turing puis le Colossus des anglais pour le déchiffrement, tel qu'évoqué dans la partie une.

Aujourd'hui, la cryptologie est toujours utilisée au niveau militaire, et s'est également élargie à un usage civil. Effectivement, si la cryptanalyse sert toujours à déchiffrer, la cryptographie assure de nouvelles fonctions telles que sur la figure 10.

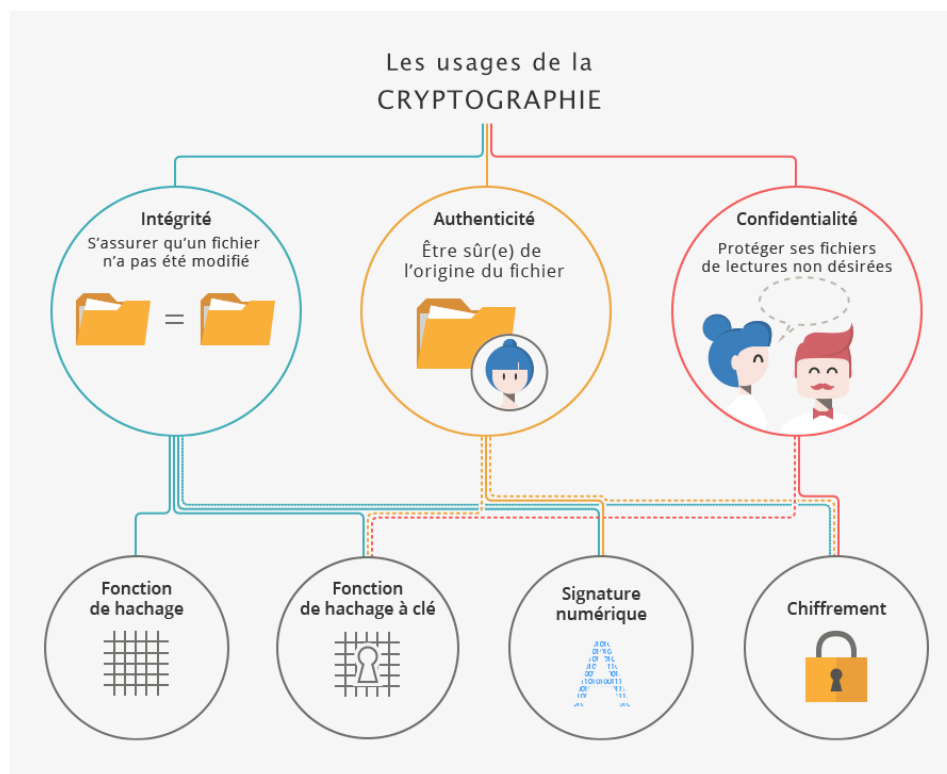


Figure 10 : Les usages de la cryptographie - CNIL - 2016

Sa première fonction est d'assurer l'intégrité d'un fichier, c'est-à-dire de pouvoir vérifier que celui-ci n'a pas été modifié. Des fonctions de hachage, des fonctions de hachage à clé, des signatures numériques et le chiffrement sont utilisés à cet effet. Une fonction de hachage est un algorithme mathématique qui mappe des données de taille arbitraire à des valeurs alphanumériques de taille fixe. Cette valeur alphanumérique est assimilable à une empreinte

²³ Larousse, 2022

numérique ainsi identifiable et vérifiable. Si la valeur alphanumérique n'est plus la même, cela veut dire que le fichier a subi des modifications. L'algorithme de hachage sécurisé SHA-1 (*Secure Hash Algorithm 1*), l'algorithme Message-Digest 5 MD5 (*Message-Digest algorithm 5*) plus anciennes, ou les algorithmes de hachage sécurisés SHA-2 et SHA-3 plus récentes sont des exemples de fonctions de hachage connues. Dans le cas des fonctions de hachage à clé, une clé secrète est échangée par les utilisateurs pour calculer l'empreinte. La sécurisation du stockage des mots de passe est réalisée à l'aide de ces fonctions. Les signatures numériques sont, elles, basées sur la cryptographie asymétrique, également connue sous le nom de cryptographie à clé publique PKC (*Public-Key Cryptography*). L'utilisation d'un algorithme à clé publique tel que Rivest-Shamir-Adleman RSA va générer une paire de clés liées mathématiquement, l'une privée et l'autre publique. Les signatures numériques fonctionnent donc grâce aux deux clés cryptographiques à authentification mutuelle de la cryptographie à clé publique. Une personne crée une signature numérique en utilisant une clé privée pour chiffrer les données liées à cette signature. Ensuite, la seule possibilité de déchiffrer les données est d'utiliser la clé publique de la personne signataire. Si le destinataire ne parvient pas à ouvrir le document avec la clé publique du signataire, cela signifie la présence d'un problème soit avec le document soit avec la signature. Finalement, il existe deux grandes familles de chiffrement, le chiffrement symétrique et le chiffrement asymétrique. Les chiffrements et déchiffrements sont basés sur l'utilisation d'une clé secrète dans le cas du chiffrement symétrique. Cela nécessite une transmission sécurisée de clés entre les parties prenantes. Tandis que le chiffrement asymétrique est basé sur la possession par le futur destinataire d'une paire de clés, l'une publique et l'autre privée et l'accessibilité aux éventuels émetteurs à sa clé publique. La clé publique du destinataire permet à l'émetteur de chiffrer le message, puis, le destinataire utilise sa clé privée pour le déchiffrer. Le chiffrement hybride combine ces deux techniques de chiffrement.

Sa deuxième fonction est de garantir l'authenticité, d'être sûr de l'origine d'un fichier. Des fonctions de hachage à clé, des signatures numériques et le chiffrement sont employés pour atteindre cet objectif.

Enfin, sa troisième fonction est de préserver la confidentialité en protégeant des données de lectures non désirées. Des fonctions de hachage à clé et le chiffrement sont exploités à cette fin.²⁴

L'ensemble de ces fonctions est actuellement effectué à l'aide des ordinateurs numériques. La sécurité est donc intrinsèquement liée aux capacités et notamment à la puissance de calcul de ces derniers.

3.2 Les changements en cryptanalyse

Aujourd'hui, les techniques de cryptographie à clé publique reposent essentiellement sur deux problèmes mathématiques. Ceux-ci sont dimensionnés afin d'être pratiquement impossibles à résoudre avec les ressources informatiques et les connaissances mathématiques actuelles. Il s'agit de la factorisation des grands nombres et du calcul du logarithme discret. Bien que tout nombre entier ait une décomposition unique en un produit de nombres premiers, trouver les facteurs premiers est donc considéré comme un problème difficile. Ainsi, la sécurité de nos transactions en ligne repose sur l'hypothèse qu'il est pratiquement impossible de factoriser des nombres entiers de mille chiffres ou plus. Cette hypothèse a été contestée en 1995 lorsque Peter Shor a proposé un algorithme quantique en temps polynomial pour le problème de factorisation. L'algorithme de Shor est sans doute l'exemple le plus spectaculaire de la façon dont le paradigme de l'informatique quantique a changé notre perception des problèmes qui devraient être considérés comme traitables.²⁵

²⁴ Commission nationale de l'informatique et des libertés (CNIL), 2016

²⁵ IBM, 2022

L'algorithme de Shor est composé de trois phases successives ; la découverte de l'ordre, la découverte de la période puis la factorisation. La figure 11 qui compare les algorithmes de factorisation classiques à l'algorithme de Shor, est une bonne illustration de ce changement de paradigme.

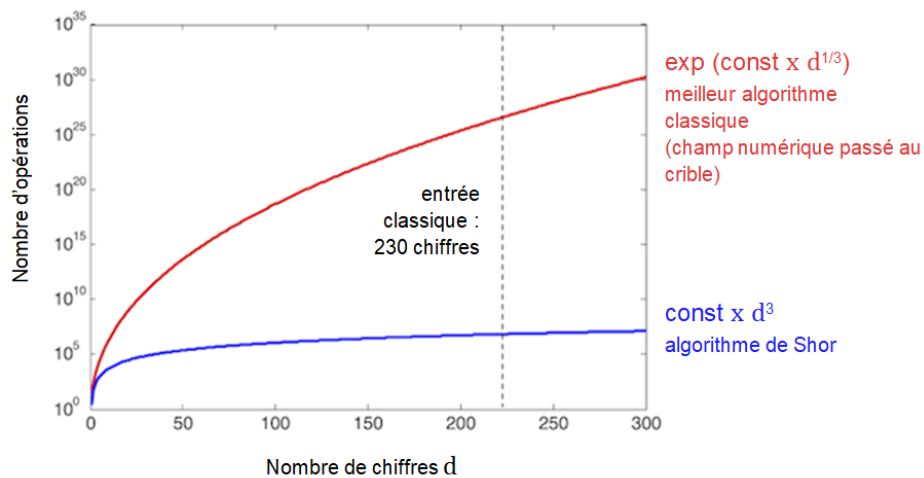


Figure 11 : Algorithmes de factorisation classiques versus algorithmes quantiques - IBM - 2020

En effet, pour un même nombre de chiffres, le nombre d'opérations à réaliser avec un algorithme de factorisation classique est exponentiel tandis qu'avec l'algorithme de Shor, il devient un simple problème presque linéaire. Les propriétés quantiques inhérentes aux ordinateurs quantiques telles que la superposition et l'intrication, sont associées à des algorithmes quantiques, qui tirent parti de ces propriétés. Ces algorithmes raccourcissent de cette façon le calcul mathématique et peuvent par conséquent casser la cryptographie actuelle. L'expérience de factorisation du nombre 15 a montré que l'informatique quantique est plus qu'une simple expérience de pensée intéressante. Il est ainsi possible d'exercer suffisamment de contrôle sur les systèmes quantiques pour exécuter des centaines d'opérations complexes et générer des résultats significatifs.²⁶

Après l'algorithme de Shor qui est le plus connu, c'est l'algorithme de Grover qui suscite l'inquiétude. Il a essentiellement prouvé que la découverte de la réponse à tout problème de recherche ou mathématique non structuré ou non ordonné peut être trouvée beaucoup plus rapidement avec les ordinateurs quantiques qu'avec les ordinateurs binaires classiques traditionnels. Grover a déclaré qu'au lieu d'avoir à calculer toutes les N solutions possibles, une à la fois, linéairement, comme cela était nécessaire sur les ordinateurs classiques, cela pouvait être fait dans la racine carrée de N sur les ordinateurs quantiques avec $\log(N) + 1$ qubits. L'algorithme de Grover fournit une accélération quadratique de la charge de travail. Il peut ainsi aider à casser les clés cryptographiques symétriques, et asymétriques dans une bien moindre mesure. Il peut aussi permettre de résoudre certains types de fonctions de hachage cryptographiques beaucoup plus rapidement sur les ordinateurs quantiques que sur les ordinateurs classiques. D'autres algorithmes créés depuis sont présentés comme étant encore plus rapides que celui de Shor, notamment une version quantique de la méthode de factorisation de courbe elliptique d'Edwards GEECM (*Grover Edwards Elliptic-Curve Factorization Method*). Il utilise l'algorithme de Grover pour à peu près doubler la longueur des nombres premiers trouvés par rapport à la méthode des courbes elliptiques d'Edwards EECM (*Edwards Elliptic-Curve Factorization Method*) standard. En supposant qu'il dispose d'un ordinateur quantique avec suffisamment de qubits et d'une vitesse comparable à l'ordinateur classique exécutant l'EECM. Cela signifie que l'algorithme de Shor est essentiellement un point de départ concernant la vitesse à laquelle les grandes équations de

²⁶ Roger A. Grimes, 2020, pages 59-85

nombre premiers peuvent être factorisées. Il est très probable qu'elles peuvent être résolues encore plus rapidement ou avec moins de qubits que prévu par Shor.

Néanmoins, les ordinateurs quantiques ne seront pour l'instant pas accessibles au tout venant. Certains fabricants prévoient notamment de limiter l'utilisation de ces derniers via l'informatique en nuage. De plus, pour contrer l'algorithme de Grover, les experts recommandent de doubler la taille des clés symétriques et des hachages afin de conserver leur relative protection dans le monde post-quantique. Par exemple, l'algorithme standard de chiffrement avancé AES (*Advanced Encryption Standard*) devra être utilisé avec une taille de clé de 256 bits pour ne pas voir sa sécurité diminuée. Il faut malgré tout se préparer, c'est pourquoi les recherches sont très actives sur le sujet et des conventions internationales réunissant des experts ont lieu régulièrement depuis 2006. Il est également nécessaire de diffuser l'information et de former dès à présent.²⁷

3.3 Les avancées en cryptographie

Si l'arrivée des ordinateurs quantiques va produire de grands changements en cryptographie, elle va aussi permettre des avancées avec le développement de nouvelles techniques. Elle va offrir ainsi une solution alternative au problème de la distribution des clés avec la distribution de clés quantiques QKD (*Quantum Key Distribution*). Cette dernière fait l'objet de nombreuses recherches depuis plusieurs années. Plusieurs normes et standards ont déjà été établis sur la QKD tels qu'évoqués au point deux de cette étude.

Le premier algorithme QKD, le protocole BB84, a été créé par l'Américain Charles Bennett et le Canadien Gilles Brassard en 1984. BB84 était le premier algorithme à montrer mathématiquement que l'utilisation d'états quantiques était à l'abri des écoutes. En effet, en omettant les détails mathématiques, si Alice veut envoyer un message à Bob sur un canal non fiable. Alice doit obtenir une clé symétrique partagée avec Bob afin qu'ils puissent commencer à chiffrer les messages secrets les uns aux autres. De façon simplifiée, voici les étapes de base du protocole BB84 :

1. Alice crée deux chaînes binaires aléatoires, disons a et b , puis les encode à l'aide de qubits et de l'algorithme mathématique BB84 en un seul résultat, disons $n.a$ et b sont mathématiquement liés l'un à l'autre, mais personne ne peut savoir ce qu'est b sans d'abord savoir ce qu'est a .
2. Alice envoie n sur un canal quantique sous forme de qubits à Bob, et c'est la dernière fois que le canal quantique est utilisé. Les communications restantes se font sur une chaîne classique publique.
3. Bob mesure tous les n qubits reçus, ce qui décohère les qubits en bits, en effet, les qubits perdent leur cohérence lors d'une mesure, cela veut dire qu'ils ne sont plus stables. Cet état de cohérence est nécessaire pour réaliser des calculs. Bob mesure donc la moitié des qubits d'une manière, disons la méthode 1, et la moitié des qubits d'une autre manière, disons la méthode 2. Seule l'une des méthodes est la bonne méthode pour ce qu'Alice a envoyé. La méthode 1 et la méthode 2 donnent des réponses différentes lors de la mesure selon que le qubit représente un 0 ou un 1. La bonne méthode qui s'aligne sur ce qu'Alice a envoyé mesurera correctement tous les 100 % de sa moitié des qubits, c'est-à-dire 50 % du total, et la mauvaise méthode finira par mesurer correctement 50 % de sa moitié des qubits, c'est-à-dire 25 % supplémentaires du total. Si Bob a reçu et mesuré correctement tous les qubits d'Alice, en raison de la façon dont ils sont mesurés, en utilisant à la fois la bonne et la mauvaise méthode, seuls 75% des bits représenteront avec précision les qubits envoyés par Alice. Ce qui est prévu.
4. Bob communique à Alice quelle méthode, 1 ou 2, il a utilisée pour mesurer chaque qubit.

²⁷ Roger A. Grimes, 2020, pages 181-183

5. Alice, sachant maintenant quelle méthode Bob a utilisée pour chaque qubit et quel aurait été le résultat, dit à Bob quels sont les qubits qu'il a mesurés qui ont été mesurés correctement et lesquels ont été mesurés de manière incorrecte.

6. Alice et Bob supprimeront tous les deux les bits incorrectement convertis, et les 75% restants deviendront leur clé secrète partagée.

7. Juste avant d'utiliser la clé secrète nouvellement partagée pour les futures communications de confiance, Alice et Bob partageront une courte série de bits de la clé entre eux sur le canal non fiable. Si la comparaison de test correspond à 100 %, ils commenceront à communiquer en toute sécurité en utilisant le reste de la clé partagée. Sinon, ils supposeront la présence de bruit ou d'écoute clandestine et ne pourront pas faire confiance à la clé partagée actuellement.²⁸

La figure 12 décrit le flux de ces différentes phases de la distribution de clé quantique.

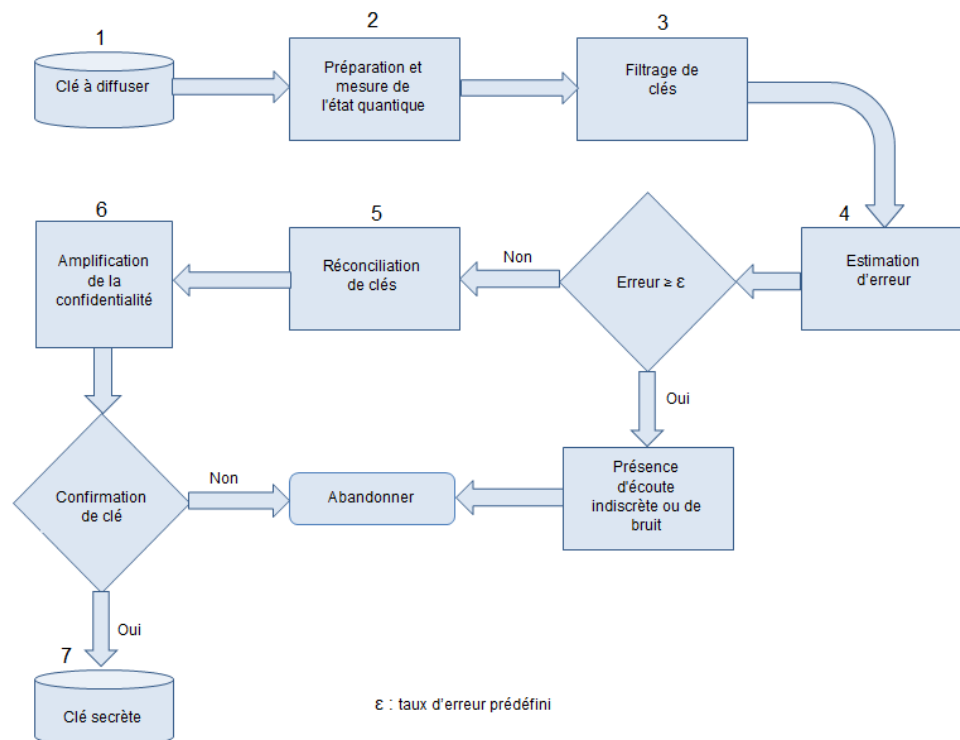


Figure 12 : Phases de distribution des clés quantiques - Nirbhay Kumar Chaubey, Bhavesh B. Prajapati - 2020

Alice et Bob ont des bits quantiques qu'ils mesurent en utilisant différents angles de polarisation. Pour générer la clé secrète, leurs résultats de mesures doivent être identiques et, au cours du processus, certains bits sont supprimés lors du processus de filtrage. Le taux d'erreur est calculé après le filtrage et si le taux d'erreur est supérieur au seuil prédéfini, le processus de distribution des clés sera abandonné. Cela peut être dû à la présence d'écoutes indiscrètes ou à une quantité de bruit plus élevée. Si le taux d'erreur est inférieur au seuil, une amplification de la confidentialité est effectuée pour réduire davantage le gain d'informations par l'écoute clandestine. La sécurité du protocole BB84 peut être comprise avec la compréhension du théorème d'absence de clonage. La présence d'un indiscret peut être détectée en observant le taux d'erreur quantique sur les bits QBER (*Quantum Bit Error Rate*) et en décidant de la valeur de QBER en quantifiant la probabilité d'un indiscret d'obtenir des informations. En 1991, le professeur anglo-polonais Artur Eker a introduit une approche QKD fondamentalement différente du protocole BB84 en utilisant l'intrication. Mais la clé secrète résultante ne serait pas fiable. L'approche QKD d'Eker, également connue

²⁸ Roger A. Grimes, 2020, pages 181-183

sous le nom de E91, a ensuite conduit à de nouveaux algorithmes QKD et d'autres procédés connexes.

La théorie de la cryptographie quantique est suffisamment mature pour fournir des preuves pour différents algorithmes, mais la mise en œuvre pratique commerciale dans la vie réelle n'est pas encore prête. Des problèmes importants doivent être pris en compte lors de la mise en œuvre des systèmes QKD. En effet, le taux d'erreur binaire est significativement élevé par rapport à un système de communication classique. Cela peut affecter la précision des opérations dans des situations pratiques. Ensuite, le canal quantique est un canal spécial qui relie deux parties point à point. Les deux parties doivent être là au bout du canal avec leur source de photons et leur détecteur. Le type de lien point à point augmente les risques de déni de service. Si un tiers n'est pas en mesure d'intercepter les messages et de rompre le lien, les parties légitimes ne peuvent même pas communiquer. Puis, il faut savoir que la QKD ne fournit pas d'authentification en soi. Il est possible d'avoir recours aux techniques actuelles. Celles-ci sont utilisées pour fournir une authentification pour la préposition de clés secrètes qui est appliquée dans un schéma d'authentification basé sur le hachage. Une approche hybride peut également être envisagée. Le prépositionnement des clés nécessite de partager les clés avant que la distribution de clé ne commence et doit encore une fois dépendre des approches traditionnelles et classiques de la distribution des clés. Le système public classique quantique hybride s'accompagne également des contraintes du système classique et des problèmes de sécurité connexes.

La question de rapidité de livraison des clés se pose aussi. Les systèmes de distribution de clés doivent fournir les clés à la vitesse requise conformément aux exigences des dispositifs de chiffrement utilisés, sinon ils pourraient être épuisés pour leurs besoins d'entrée. Les derniers systèmes QKD peuvent atteindre un débit allant jusqu'à 1000 bits/seconde dans le cas idéal. Le taux réel peut même être très bas. Enfin, il existe un problème d'indépendance de la distance et de l'emplacement. Effectivement, dans le cas d'une distribution de clé classique, toute partie peut convenir ou transférer des clés à n'importe quelle distance ou depuis n'importe quel endroit en utilisant des protocoles Internet. Ce n'est pas possible avec la distribution de clé quantique. Le cadre Internet sous-jacent qui peut communiquer des photons à distance et à différents endroits est encore à un niveau très primaire et limité à quelques kilomètres utilisant la fibre. Il est probable que l'architecture hybride doit être appliquée et à un certain niveau l'interface avec le monde classique doit être fournie.

Dans le cadre de la cryptographie quantique, il existe également des générateurs de nombres aléatoires quantiques et des chiffrements quantiques. Ce n'est très probablement que le début des avancées en cryptographie. Comme pour l'ensemble des domaines du quantique, des équipes pluridisciplinaires vont être nécessaires pour la cryptologie, et là aussi, il va falloir informer et former.²⁹

Enfin, d'après l'Agence Nationale de la Sécurité des Systèmes d'Information, l'ANSSI, il est important de reconnaître l'immaturité de la cryptographie post-quantique. L'ANSSI n'approuvera aucun remplacement direct des algorithmes actuellement utilisés à court/moyen terme. Cependant, cette immaturité ne doit pas servir d'argument pour reporter les premiers déploiements. L'ANSSI encourage donc toutes les industries à commencer une transition en utilisant de façon concomitante la cryptographie classique et la cryptographie quantique. Ceci afin d'augmenter progressivement la confiance dans les algorithmes post-quantiques et leurs implémentations. Cela permettrait aussi de s'assurer qu'il n'y a pas de régression de la sécurité en ce qui concerne la sécurité classique. Ainsi, l'ANSSI recommande de mettre en place dès que possible la défense en profondeur post-quantique pour les produits de sécurité visant à offrir une protection durable des informations jusqu'après 2030 ou qui seront potentiellement utilisés après 2030.³⁰

²⁹ Nirbhay Kumar Chaubey, Bhavesh B. Prajapati, 2020

³⁰ ANSSI, 2022

CONCLUSION

Dans cette étude, le panorama des différentes générations d'ordinateurs a permis d'identifier quatre grandes générations d'ordinateurs ; les calculateurs mécaniques, les ordinateurs analogiques, les ordinateurs numériques et les ordinateurs quantiques. Les récentes avancées pour la dernière génération des ordinateurs quantiques, se caractérisent par plus de puissance, un retour à l'informatique centralisée et, au final, à une forme de fonctionnement « analogique » ou pour le moins basé sur une grandeur physique : le phénomène quantique.

En revanche, en matière d'informatique quantique, les plus importantes problématiques sont l'impossibilité à ce jour d'interpréter directement les résultats produits par un ordinateur quantique, ainsi que l'incapacité à stocker les données. C'est pourquoi les architectures quantiques actuelles contournent cette problématique à l'aide d'une passerelle d'interconnexion vers l'informatique numérique ; ce qui constitue un assemblage de systèmes informatiques hétérogènes « quantique-numérique ».

Néanmoins, des progrès sont réalisés à des vitesses extraordinaires au niveau mondial. Les normes et standards sont encore en pleine évolution. Car en réalité, les fabricants sont encore en phase de recherche et développement, donc dans une grande liberté de choix en matière de conception et d'architecture.

Preuve en est que le travail de standardisation de l'ETSI en Europe sur la distribution de clé quantique, ainsi que le focus sur un cas d'application d'ordinateur quantique en cryptologie confirment la réalité de l'ordinateur quantique. En effet, l'arrivée des ordinateurs quantiques va vraiment révolutionner la cryptanalyse et la cryptographie.

Ainsi, pour l'instant, la suprématie quantique n'est pas encore atteinte et les ordinateurs quantiques sont surtout utilisés dans des domaines très spécifiques. D'autant plus qu'il est nécessaire d'avoir recours à des équipes d'ingénieurs spécialisés et pluridisciplinaires.

Finalement, seul un abaissement des coûts ou des solutions de partage, avec peut-être un retour au temps partagé, permettront de rentabiliser les investissements, seule condition d'un développement en masse. Effectivement, si l'invention consiste à créer quelque chose de nouveau et d'original, l'innovation consiste à transformer cette nouveauté en un produit commercial très demandé. Comme le transistor l'a connu avec la loi de Moore, le développement exponentiel de l'ordinateur quantique pourra alors contribuer à l'explosion de la puissance de traitement informatique dans des domaines d'application les plus variés.

ANNEXES

A. LE CHAT DE SCHRÖDINGER

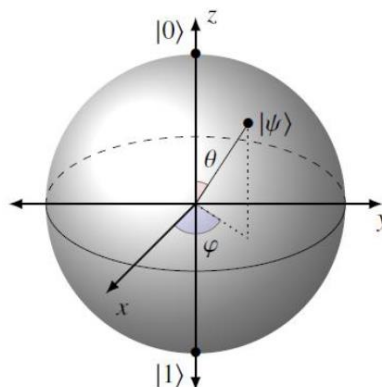
Laboratoire de physique atomique de l'état solide, Université de Cornell, New York, Le chat de Schrödinger <https://www.lassp.cornell.edu/ardlouis/dissipative/Schrcat.html> 31/05/1994, consulté le 22/04/2022

Un chat, un flacon de poison et une source radioactive sont placés dans une boîte scellée. Si un moniteur interne (par exemple un compteur Geiger) détecte la radioactivité (c'est-à-dire la décomposition d'un seul atome), le flacon est brisé, libérant le poison, qui tue le chat. L'interprétation de Copenhague de la mécanique quantique implique qu'après un certain temps, le chat est simultanément vivant et mort. Pourtant, quand on regarde dans la boîte, on voit le chat vivant ou mort, pas à la fois vivant et mort. Cela pose la question de savoir quand exactement la superposition quantique se termine et la réalité se résout en une possibilité ou une autre. Ce chat hypothétique peut donc être considéré à la fois vivant et mort du fait que son destin est lié à un événement subatomique aléatoire qui peut ou non se produire. Cette expérience de pensée permet de démontrer la complexité de la théorie quantique et que de simples interprétations erronées peuvent conduire à des résultats absurdes qui ne correspondent pas au monde réel.

B. PRINCIPE DE FONCTIONNEMENT DES QUBITS

Robert S. Sutor, Dancing with Qubits How quantum computing works and how it can change the world, Packt Publishing Birmingham, ISBN 978-1-83882-736-6, 2019, pages 2-4, 248-252

Un Qubit est représenté de façon standard par la sphère de Bloch. Cette sphère a été nommée d'après Félix Bloch, un scientifique qui a remporté le prix Nobel de physique en 1962 pour son travail sur la résonance magnétique nucléaire.



Sphère de Bloch © Robert S. Sutor, Dancing with Qubits How quantum computing works

Avec un qubit, la terminologie allumé ou éteint, 1 ou 0, est remplacée respectivement par $|1\rangle$ et $|0\rangle$. En mécanique quantique, cette notation nommée bra-ket a été introduite par Dirac et permet d'indiquer que l'on superpose des états. Dirac l'a créée afin de faciliter l'écriture des équations de la mécanique quantique, ainsi que pour souligner l'aspect vectoriel de l'objet représentant un état quantique. Dans le diagramme de la sphère de Bloch, la position du qubit est déterminée par deux angles θ et φ . Le vecteur $|\psi\rangle$ représente l'état quantique d'un qubit. De façon naturelle, l'état $|0\rangle$ a une probabilité de 1.0 de se produire lui-même lorsqu'il est mesuré et la probabilité 0.0 de produire $|1\rangle$. Ces probabilités sont inversées pour l'état






$|1\rangle$. Pour une latitude sur la sphère de Bloch qui n'est pas l'équateur, les probabilités de chuter à $|0\rangle$ ou $|1\rangle$ sont différentes mais sont toujours des additions jusqu'à 1.0. La probabilité de produire $|0\rangle$ est la même pour chaque point de cette latitude, de même pour $|1\rangle$. La valeur du qubit est déterminée par des combinaisons d'une propriété binaire appelée spin. Si le spin est haut pour un électron alors qu'il est « bas » pour le noyau, dans ce cas, le qubit a une valeur globale de 1. Dans le cas inverse, le qubit a une valeur globale de 0.

C. LES PORTES LOGIQUES D'UN ORDINATEUR QUANTIQUE








IBM, Glossaire des opérations, consulté le 22/04/2022

https://quantum-computing.ibm.com/composer/docs/ibmq/operations_glossary#rc3x-gate


Les portes classiques du circuit d'un ordinateur quantique :

Symbole	Nom	Traitement
	Porte NOT ou Porte Pauli X	Renverse l'état $ 0\rangle$ à $ 1\rangle$, et vice versa
	Porte contrôlée-NOT ou Porte contrôlée-x (CX)	Agit sur une paire de qubits, l'un agissant comme « contrôle » et l'autre comme « cible ». Elle effectue un NOT sur la cible chaque fois que le contrôle est dans l'état $ 1\rangle$. Si le qubit de contrôle est en superposition, cette porte crée une intrication.
	Porte de Toffoli ou Double porte NON contrôlée (CCX)	Possède deux qubits de contrôle et une cible. Elle applique un NOT à la cible uniquement lorsque les deux contrôles sont dans l'état $ 1\rangle$.
	Porte SWAP	Echange les états de deux qubits.
	Porte d'identité ou Porte Id ou Porte I temps de porte.	Est en fait l'absence de porte. Elle garantit que rien n'est appliqué à un qubit pendant une unité de temps de porte.











Les portes de phase du circuit d'un ordinateur quantique :

Symbole	Nom	Traitement
	Porte T	Les ordinateurs quantiques tolérants aux pannes compileront tous les programmes quantiques jusqu'à la porte T et son inverse, ainsi que les portes Clifford.
	Porte S	Applique une phase de i à l'état $ 1\rangle$.
	Porte Pauli Z	Agit comme identité sur l'état $ 0\rangle$ et multiplie le signe de l'état $ 1\rangle$ par -1. Elle inverse donc les états $ +\rangle$ et $ -\rangle$. Dans la base $ +\rangle, -\rangle$, elle joue le même rôle que la porte NOT dans la base $ 0\rangle, 1\rangle$.
	Porte Tdg ou T-dagger	Effectue l'inverse de la porte T.
	Porte Sdg ou S-dagger	Effectue l'inverse de la porte S.
	Porte Phase (précédemment appelée porte U1)	Applique une phase de $e^{i\theta}$ à l'état $ 1\rangle$. Pour certaines valeurs de θ , elle est équivalente à d'autres portes.
	Porte RZ	Exécute $\exp(-i\frac{\theta}{2}Z)$. Sur la sphère de Bloch, cette porte correspond à la rotation de l'état du qubit autour de l'axe z de l'angle donné.






La porte d'Hadamard du circuit d'un ordinateur quantique :

Symbole	Nom	Traitement
	Porte Hadamard ou Porte H	Fait tourner les états $ 0\rangle$ et $ 1\rangle$ à $ +\rangle$ et $ -\rangle$, respectivement. C'est utile pour faire des superpositions. Si une porte universelle est définie sur un ordinateur classique et que la porte Hadamard est ajoutée, elle devient une porte universelle définie sur un ordinateur quantique.

Les portes quantiques du circuit d'un ordinateur quantique :

Symbole	Nom	Traitement
	Porte \sqrt{X} ou porte NON à racine carrée	Implémente la racine carrée de X , \sqrt{X} . L'application de cette porte deux fois de suite produit la porte Pauli-X standard (NOT gate). Comme la porte Hadamard, \sqrt{X} crée un état de superposition égal si le qubit est dans l'état $ 0\rangle$, mais avec une phase relative différente. Sur certains matériels, il s'agit d'une porte native qui peut être implémentée avec une impulsion $\pi/2$ ou X90.
	Porte \sqrt{X}^\dagger ou Porte SXdg ou Porte NOT-dagger à racine carrée	Est l'inverse de la porte \sqrt{X} . L'appliquer deux fois de suite produit la porte Pauli-X (porte NON), puisque la porte NON est son propre inverse.
	Porte Y ou Porte Pauli Y	Est équivalente à R_y pour l'angle π . Cela revient à appliquer X et Z, à un facteur de phase global près.
	Porte RX	Exécute $\exp(-i\frac{\theta}{2}X)$. Sur la sphère de Bloch, cette porte correspond à la rotation de l'état du qubit autour de l'axe x de l'angle donné.
	Porte RY	Exécute $\exp(-i\frac{\theta}{2}Y)$. Sur la sphère de Bloch, cette porte correspond à la rotation de l'état du qubit autour de l'axe y de l'angle donné et n'introduit pas d'amplitudes complexes.
	La porte RXX	Exécute $\exp(-i\frac{\theta}{2X} \otimes X)$.
	Porte RZZ	Nécessite un seul paramètre : un angle exprimé en radians. Cette porte est symétrique ; échanger les deux qubits sur lesquels elle agit ne change rien.
	Porte en U (Auparavant appelée la porte U3)	Les trois paramètres permettent la construction de n'importe quelle porte à un seul qubit. A une durée d'une unité de temps de porte.
	Porte Toffoli simplifiée ou Porte Margolus	Implémente la porte de Toffoli jusqu'aux phases relatives. Cette implémentation nécessite trois portes CX, ce qui est le minimum possible
	Porte RC3X ou Porte Toffoli simplifiée à 3 commandes.	Implémente la porte de Toffoli jusqu'aux phases relatives. Le Toffoli simplifié n'est pas équivalent au Toffoli, mais peut être utilisé dans des endroits où la porte de Toffoli n'est à nouveau pas calculée.

Les opérateurs et modificateurs non unitaires du circuit d'un ordinateur quantique :

Symbole	Nom	Traitement
	Opération de réinitialisation	Renvoie un qubit à l'état $ 0\rangle$, quel que soit son état avant l'application de l'opération. Ce n'est pas une opération réversible.
	Mesure dans la base standard ou Base z ou Base de calcul	Peut être utilisé pour mettre en œuvre tout type de mesure lorsqu'il est combiné avec des portes. Ce n'est pas une opération réversible.
	Modificateur de contrôle	Donne une porte dont le fonctionnement d'origine dépend maintenant de l'état du qubit de contrôle. Lorsque le contrôle est dans l'état $ 1\rangle$, le(s) qubit(s) cible(s) subissent l'évolution unitaire spécifiée. En revanche, aucune opération n'est effectuée si la commande est dans l'état $ 0\rangle$. Si la commande est dans un état de superposition, alors l'opération résultante découle de la linéarité.
	IF	Permet d'appliquer conditionnellement des portes quantiques, en fonction de l'état d'un registre classique.
	Fonctionnement de la barrière	Pour rendre un programme quantique plus efficace, le compilateur essaiera de combiner des portes. La barrière est une instruction au compilateur pour empêcher ces combinaisons d'être faites. De plus, il est utile pour les visualisations.

REFERENCES

1. **France culture**, Article : « Ordinateurs et communication quantiques : la découverte d'un matériau prometteur », du 10/03/2022, consulté le 04/04/2022
<https://www.franceculture.fr/emissions/le-journal-des-sciences/le-journal-des-sciences-du-jeudi-10-mars-2022>
2. **Zdnet**, Article « Google affirme que l'informatique quantique arrivera dans la décennie à venir », du 05/01/2022, consulté le 04/04/2022
<https://www.zdnet.fr/actualites/google-affirme-que-l-informatique-quantique-arrivera-dans-la-decennie-a-venir-39934999.htm>
3. **Le Monde**, Article « La cryptographie se prépare non sans peine à l'avènement de l'ordinateur quantique », du 06/03/2022, consulté le 04/04/2022
https://www.lemonde.fr/sciences/article/2022/03/06/la-cryptographie-se-prepare-non-sans-peine-a-l-avenement-de-l-ordinateur-quantique_6116374_1650684.html
4. **Dictionnaire Larousse en ligne**, Définition : ordinateur, consulté le 10/05/2022
<https://www.larousse.fr/dictionnaires/francais/ordinateur/56358>
5. **CIGREF**, Ainsi naquit le mot « ordinateur », 09/08/2011, consulté le 10/05/2022
<https://www.cigref.fr/archives/histoire-cigref/blog/ainsi-naquit-le-mot-ordinateur/>
6. **Simson L. Garfinkel, Rachel H. Grunspan**, *The computer book, from the Abacus to artificial intelligence*, 250 milestones in the history of computer science, Sterling, New York, ISBN 978-1-4549-2622-1, 2018, pages 23-31
7. **Georges Ifrah**, *The universal history of computing, from the Abacus to the quantum computer*, John Wiley & Sons, New York, ISBN 0-471-39671-0, 2001, pages 122-125
8. **Simson L. Garfinkel, Rachel H. Grunspan**, *The computer book, from the Abacus to artificial intelligence*, 250 milestones in the history of computer science, Sterling, New York, ISBN 978-1-4549-2622-1, 2018, pages 30-31, 127-131
9. **Sacha Krakowiak**, « Le modèle d'architecture de von Neumann », 18/11/2011 consulté le 11/05/2022 <https://interstices.info/le-modele-darchitecture-de-von-neumann/>
10. **Alain Brochier, François Rechenmann**, Les calculateurs analogiques, 31/03/2008, consulté le 17/05/2022 <https://interstices.info/les-calculateurs-analogiques/>
11. **Claude Chevassu**, professeur de génie électrique, Ecole Nationale Supérieure Maritime Marseille, Site consacré à l'électricité et aux machines électriques, consulté le 14/05/2022
http://mach.elec.free.fr/divers/portes_analogiques.doc
12. **Luc De Mey**, Les portes logiques de base, 2022, Consulté le 14/05/2022
<https://courstechinfo.be/Techno/PortesLogiques.pdf>
13. **Gordon E. Moore**, Director, Research and Development Laboratories, Fairchild Semiconductor division of Fairchild Camera and Instrument Corp., Electronics, Volume 38, Number 8, April 19, 1965, Intel Corporation, 2005
https://hasler.ece.gatech.edu/Published_papers/Technology_overview/gordon_moore_1965_article.pdf

14. **Simson L. Garfinkel, Rachel H. Grunspan**, *The computer book, from the Abacus to artificial intelligence, 250 milestones in the history of computer science*, Sterling, New York, ISBN 978-1-4549-2622-1, 2018, pages 540-541
15. **IBM**, « Power 4 », The First Multi-Core, 1GHz Processor 2022, consulté le 11/05/2022
<https://www.ibm.com/ibm/history/ibm100/us/en/icons/power4/>
16. **Jon Fortt**, Live: Moira Gunn interviews Gordon Moore at Intel Developer Forum, 19/09/2007, consulté le 16/04/2022
<https://fortune.com/2007/09/18/live-moira-gunn-interviews-gordon-moore-at-intel-developer-forum/>
17. **Simson L. Garfinkel, Rachel H. Grunspan**, *The computer book, from the Abacus to artificial intelligence, 250 milestones in the history of computer science*, Sterling, New York, ISBN 978-1-4549-2622-1, 2018, pages 687-688
18. **Antonio Acín et al.**, « The European Quantum Technologies Roadmap », 12/12/2017, consulté le 11/05/2022 <https://arxiv.org/abs/1712.03773>
19. **Dr. Gopala Krishna Behara**, Lead Enterprise Architect Wipro Technologies, « Overview of Quantum Computer Platform », 13/09/2021 consulté le 22/04/2022
<https://www.analyticsinsight.net/overview-of-quantum-computer-platform/>
20. **IBM**, « The Quantum Decade », 2021 consulté le 09/05/2022
<https://www.ibm.com/downloads/cas/J25G35OK>
21. **Institut des ingénieurs électriciens et électroniciens (IEEE)**, consulté le 22/04/2022
<https://quantum.ieee.org/standards>
22. **Institut européen des normes de télécommunications (ETSI)**, consulté le 23/04/2022
<https://www.etsi.org/>
23. **Dictionnaire Larousse**, Définition : cryptologie, consulté le 28/04/2022
<https://www.larousse.fr/dictionnaires/francais-monolingue>
24. **Site web de la Commission nationale de l'informatique et des libertés (CNIL)**, « Comprendre les grands principes de la cryptologie et du chiffrement », 25/10/2016, consulté le 01/05/2022
<https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>
25. **IBM**, « L'algorithme de Shor », consulté le 03/05/2022
<https://quantum-computing.ibm.com/composer/docs/idx/guide/shors-algorithm>
- 26, 27, 28. **Roger A. Grimes**, *Cryptography Apocalypse, Preparing for the Day When Quantum Computing Breaks Today's Crypto*, John Wiley & Sons, New Jersey, ISBN 978-1-119-61819-5, 2020, pages 59-85 (26), 181-183 (27, 28)
29. **Nirbhay Kumar Chaubey, Bhavesh B. Prajapati**, *Quantum Cryptography and the Future of Cyber Security*, IGI Global Hershey, ISBN 9781799822530, 2020, pages 98-105
30. **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)**, « ANSSI views on the Post-Quantum Cryptography transition », 04/01/2022, consulté le 05/05/2022
<https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/>

Les ordinateurs quantiques

Rapport pour l'obtention de l'UE ENG221 « Information et communication pour l'ingénieur »
Spécialité informatique.

C.N.A.M. Bretagne. Rennes, 2021

RESUME

Les médias parlent beaucoup des ordinateurs quantiques, mais de quoi s'agit-il concrètement ? Cette étude a pour but de donner un éclairage objectif sur le sujet. Ainsi, un panorama des différentes générations d'ordinateurs permet de comprendre le contexte d'émergence de ces derniers ; des calculateurs mécaniques ; des ordinateurs analogiques ; des ordinateurs numériques ; des ordinateurs quantique. Puis, les principes de fonctionnement et l'architecture des ordinateurs quantiques sont expliqués, et les normes et standards actuels sont abordés. Enfin, un cas d'application de cryptologie est exposé. En effet, les ordinateurs quantiques sont à même de révolutionner ce domaine. D'un côté, en cryptanalyse, les algorithmes de Shor, puis de Grover ont prouvé leur capacité à factoriser les grands nombres et du calculer les logarithmes discrets sur les ordinateurs quantiques. Or, ce sont sur ces deux problèmes mathématiques sur lesquels reposent les techniques de cryptographie à clé publique par exemple. Ceux-ci sont aujourd'hui dimensionnés afin d'être pratiquement impossibles à résoudre avec les ressources informatiques et les connaissances mathématiques actuelles, ce qui ne sera donc plus le cas avec les ordinateurs quantiques. D'un autre côté, en cryptographie, de nouvelles techniques comme la distribution de clé quantique semblent prometteuses.

Mots clés : ordinateur quantique, quantum bit, qubit, architecture quantique, normes, standards, cryptologie, cryptographie, cryptanalyse, algorithme, distribution de clé quantique (QKD)

SUMMARY

Medias talk a lot about quantum computers, but what about it in practice? This study aims to give an objective opinion on the subject. Thus, an overview of the different generations of computers; mechanical calculators; analog computers; digital computers; quantum computers, helps to understand the context of their emergence. Then, the operating principles and architecture of quantum computers are explained, and current norms and standards are discussed. Finally, a cryptology application case is exposed. Indeed, quantum computers are able to revolutionize this field. On the one hand, in cryptanalysis, the algorithms of Shor, then of Grover have proven their ability to factorize large numbers and calculate discrete logarithms on quantum computers. However, it is on these two mathematical problems on which public key cryptography techniques are based, for example. These are now sized to be practically impossible to solve with current computing resources and mathematical knowledge, which will therefore no longer be the case with quantum computers. On the other hand, in cryptography, new techniques like quantum key distribution seem promising.

Key words: quantum computer, quantum bit, qubit, quantum architecture, norms, standards, cryptology, cryptography, cryptanalysis, algorithm, quantum key distribution (QKD)