Chapitre 3
Les ordinateurs quantiques

1. Des quanta et des bits

1.1 La physique quantique

En 1900, le physicien Max Planck propose une théorie qui permet d'expliquer le rayonnement généré par un corps chauffé à une certaine température. Dans cette théorie, les transferts d'énergie ne se font pas de manière continue, mais par de petits « paquets » d'énergie, appelés « quanta ». En 1905, Albert Einstein reprend la notion de quanta d'énergie dans un article qui explique l'effet photoélectrique par lequel un corps recevant de la lumière émet des électrons. Sur cette base, de nombreux autres scientifiques, dont Niels Bohr, Louis de Broglie, Paul Dirac, Erwin Schrödinger, Wolfgang Pauli, Werner Heisenberg, Max Born, Satyendra Nath Bose et Enrico Fermi apportent leur pierre à l'édifice de la physique quantique, qui permet de décrire et de prédire les phénomènes se déroulant à l'échelle des atomes et des particules subatomiques. Elle a rendu possibles de multiples innovations technologiques à partir des années 1950, comme les transistors, les lasers, les cellules photovoltaïques ou l'imagerie par résonance magnétique (IRM). La physique quantique connaît une nouvelle phase de développement dans les années 1980, nommée la « seconde révolution quantique », lorsque des scientifiques réussissent à isoler des objets quantiques (atomes, électrons, photons, ions), à les manipuler et à les mesurer individuellement.

La physique quantique possède deux propriétés étonnantes et contre-intuitives. La première est la superposition des états quantiques. Il est en effet possible qu'un objet quantique se trouve dans un état superposé. Là où en physique classique un objet serait, soit dans un état A, soit dans un état B, un objet peut être, en physique quantique, dans une superposition d'état A et d'état B. La seconde propriété est tout aussi surprenante : deux objets quantiques peuvent être « intriqués ». Leurs états quantiques sont alors liés, quelle que soit la distance qui les sépare.

1.2 L'ordinateur quantique

L'idée d'un ordinateur tirant parti des propriétés déroutantes de la physique quantique apparaît durant les années 1980, quand des physiciens comme Paul Benioff, Richard Feynman et David Deutsch proposent de concevoir des ordinateurs utilisant de telles caractéristiques pour simuler des systèmes physiques quantiques ou réaliser des calculs. Dans les années 1990, alors que l'ordinateur quantique est encore purement théorique, des mathématiciens créent des algorithmes quantiques et montrent leurs avantages par rapport à ceux fonctionnant sur des ordinateurs classiques.

Dans un ordinateur classique, l'information est stockée et traitée sous forme de bits. À un instant donné, un bit ne peut avoir qu'une valeur, soit 0, soit 1. Dans un ordinateur quantique, l'unité fondamentale d'information est le bit quantique, ou « qubit ». Ces qubits sont implémentés par des objets quantiques en état superposé. Un qubit peut avoir simultanément la valeur 0 et la valeur 1, avec, quand il est mesuré, une certaine probabilité d'être dans l'état 0 et une certaine probabilité d'être dans l'état 1. Cela permet de concevoir des algorithmes où l'on fait subir à un ensemble de qubits superposés une succession d'opérations logiques mises en œuvre physiquement en soumettant les objets quantiques sous-jacents à des lasers ou des micro-ondes. Ces opérations sont appelées « portes quantiques ». Le passage par une porte quantique modifie l'état des qubits tout en conservant la superposition des états. À la fin du calcul, des mesures sont faites sur les qubits, ce qui les fait sortir de leur état superposé et donne le résultat final. Le principe d'un algorithme quantique est d'appliquer des opérations sur les qubits pour les faire converger, tout en maintenant la superposition, vers des états fournissant les valeurs attendues à l'issue de l'exécution du programme. Certains algorithmes quantiques sont

probabilistes, ce qui signifie qu'il faut les lancer plusieurs fois pour obtenir un résultat suffisamment précis.

Le principal avantage de l'ordinateur quantique est de pouvoir résoudre certains problèmes beaucoup plus rapidement que des ordinateurs classiques. Il existe en effet des problèmes que l'on sait traiter en théorie, mais pas en pratique. Des algorithmes permettant d'en trouver les solutions ont été conçus, mais les temps de calcul sur un ordinateur classique augmentent de façon exponentielle avec la dimension du problème. Un exemple est celui du voyageur de commerce qui doit passer dans N villes et qui veut ne passer qu'une fois dans chaque ville. Si la taille du problème est petite, l'ordinateur peut exécuter l'algorithme en quelques secondes ou minutes. Mais si la taille du problème est importante, le temps de calcul devient démesuré car il se compte en années voire en dizaines, centaines, milliers ou millions d'années, même si un grand nombre d'ordinateurs très puissants est mobilisé. Or, certains de ces problèmes peuvent être résolus par des algorithmes quantiques s'exécutant en quelques secondes, minutes ou heures de calcul. Un cas d'usage très prometteur est celui de la simulation de grosses molécules qui permettrait des avancées majeures en chimie et en pharmacologie. Des problèmes complexes d'optimisation pourraient être réglés dans des domaines comme la logistique, les transports ou les réseaux de communication ou de distribution d'énergie.

Les principes de fonctionnement d'un ordinateur quantique se heurtent pourtant à des difficultés pratiques nombreuses et ardues. Les qubits sont implémentés par le biais d'objets physiques, selon différentes techniques : circuits supraconducteurs, atomes, ions, électrons, photons. L'état de superposition quantique de ces objets est très fragile et disparaît extrêmement rapidement, du fait des interactions avec leur environnement. Ce phénomène est appelé « la décohérence ». Le temps de cohérence des qubits au sein des ordinateurs quantiques est, à la date de rédaction de ce livre, de l'ordre du millième de seconde, ce qui limite le nombre d'opérations pouvant être réalisées par les algorithmes. Pour augmenter ce temps de cohérence, les qubits sont maintenus à des températures extrêmement basses, très proches du zéro absolu, ce qui diminue les perturbations, mais qui nécessite des dispositifs de refroidissement complexes et contraignants. Un autre obstacle est le taux d'erreur constaté sur les opérations effectuées sur les qubits, ce qui peut restreindre également le nombre de portes quantiques utilisables. Pour prendre en compte ces conditions, des algorithmes de correction d'erreurs sont développés. Ils

permettent d'obtenir des qubits « logiques » à partir de plusieurs qubits « physiques ». L'avantage est que les qubits logiques ont des taux d'erreur très inférieurs à ceux des qubits physiques. L'inconvénient est qu'il faut un nombre élevé de qubits physiques pour disposer d'un seul qubit logique.

Le nombre de qubits d'un ordinateur quantique est devenu un marqueur de la maturité de la technologie des différents constructeurs. Les prototypes d'ordinateurs quantiques sont passés de quelques qubits dans les années 2000 à une petite centaine à la date de rédaction de ce livre. Les entreprises travaillant sur des ordinateurs quantiques, comme Google, Microsoft, IBM, Intel ou Rigetti, prévoient une augmentation rapide du nombre de qubits dans les années qui viennent. En mai 2022, IBM promet un ordinateur quantique de plus de 4 000 qubits pour 2025. Mais les problèmes techniques à résoudre sont épineux, les effets d'annonce ne sont pas absents et il est particulièrement difficile de prédire quand un ordinateur quantique à plusieurs milliers, voire millions de qubits, avec des taux d'erreur suffisamment bas et des temps de cohérence suffisamment longs, verra le jour.

1.3 La distribution de clefs quantique

La physique quantique permet de réaliser d'autres prouesses qui sont souvent confondues à tort avec l'ordinateur quantique. Ainsi des protocoles de distribution de clefs cryptographiques (QKD, *Quantum Key Distribution*) comme BB84 utilisent des lois de la physique quantique pour assurer le transfert sécurisé de données entre deux parties via des photons. Ces lois disent qu'il est impossible, d'une part, de mesurer un qubit sans le faire sortir de son état superposé, et, d'autre part, de cloner ou copier un qubit en état superposé. Si un adversaire veut espionner l'échange entre l'émetteur et le destinataire, il doit intercepter et mesurer l'état quantique des photons pour obtenir la clef. Le protocole est conçu pour que cette mesure génère des erreurs, qui peuvent ensuite être détectées par les deux parties légitimes. Il est, de plus, impossible à l'attaquant de cloner un photon avant de le mesurer. Les parties voulant échanger des secrets comme des clefs cryptographiques doivent donc être équipées d'appareils spécialisés reliés par un lien capable de transporter des objets quantiques, comme des photons, et par un lien classique de communication. D'autres protocoles de QKD, comme E91, sont basés sur l'intrication quantique. Ce type de technologie est déjà mature, avec des équipements vendus dans le commerce et des installations

opérationnelles entre des sites sensibles distants de quelques dizaines de kilomètres, dans le secteur bancaire principalement.

1.4 Les réseaux de communication quantiques

Un axe de recherche connexe est celui des réseaux de communication quantiques, réseaux qui rendent possible la transmission sécurisée de clefs cryptographiques et d'autres types de données sensibles entre de multiples équipements. Ils pourraient aussi acheminer des qubits entre deux appareils et permettre à plusieurs ordinateurs quantiques de s'échanger des qubits. De telles infrastructures sont basées sur le principe de la téléportation d'états quantiques, réalisée grâce à des photons intriqués. Pour avoir un véritable réseau transportant des qubits sur des milliers de kilomètres et entre de multiples nœuds, il faut mettre en œuvre des matériels de type répéteur ou routeur de confiance.

Des travaux de recherche sont en cours pour concevoir des réseaux quantiques ne nécessitant pas de tels matériels, malgré les lois physiques et les contraintes (impossibilité de mesurer un qubit dans un état superposé, impossibilité de cloner un qubit, temps de décohérence des qubits, perte des photons durant la transmission, interopérabilité, etc.) Des prototypes de réseaux quantiques constitués de quelques dizaines de nœuds existent et des expériences de communications quantiques entre des stations au sol et des satellites sont menées.

2. L'épée de Damoclès quantique

2.1 L'algorithme de Shor

En 1995, Peter Shor, un mathématicien en poste au sein des légendaires Bell Labs, publie un article [1] décrivant une méthode permettant de factoriser des nombres en leurs facteurs premiers à l'aide d'un ordinateur quantique. Aucun prototype d'ordinateur quantique n'existe alors. L'algorithme de chiffrement asymétrique RSA a été créé dix-sept ans auparavant et TLS/SSL, le protocole de sécurisation du Web qui utilise largement la cryptographie asymétrique, est en train d'apparaître avec l'Internet grand public.

La sécurité des algorithmes de chiffrement asymétrique comme RSA repose sur le fait qu'il est impossible en pratique de déterminer la clef privée à partir de la clef publique. Il faudrait factoriser un nombre extrait de la clef publique, c'est-à-dire trouver les deux nombres premiers dont ce nombre est le produit. Les temps d'exécution des meilleurs algorithmes de factorisation sur un ordinateur classique augmentent de façon sous-exponentielle, ce qui veut dire que les temps de calcul s'accroissent très rapidement avec la taille du nombre à factoriser. N'importe qui peut casser une clef RSA de 256 bits sur son ordinateur personnel, mais le dernier record en date est une clef RSA de 829 bits cassée en février 2020 après 3 mois de calcul sur plusieurs centaines de processeurs.

Casser des clefs RSA de 2 048 ou 4 096 bits avec un algorithme de factorisation sur un ordinateur classique nécessiterait des temps de calcul incroyablement longs. Le temps d'exécution de l'algorithme de Shor augmente, lui, de façon polynomiale avec la taille du nombre à factoriser, c'est-à-dire beaucoup plus lentement, ce qui rend possible le cassage de clefs privées issues d'algorithmes asymétriques basés sur les nombres premiers comme RSA. L'algorithme de Shor rend également vulnérables les algorithmes basés sur le problème du logarithme discret comme Diffie-Hellman, un algorithme d'échange de clefs, et ceux basés sur les courbes elliptiques, tels qu'ECDSA.

L'algorithme de Shor est donc une menace pour la cryptographie asymétrique. Peter Shor savait ce qu'impliquait son travail, car il cite RSA comme l'une des cibles potentielles de son algorithme. Sont concernés les algorithmes de signature électronique utilisés dans des processus d'authentification, de paiement ou de certification de documents, et les algorithmes d'échange de clefs symétriques ensuite employés pour chiffrer des données ou établir des canaux de communication sûrs. Ces algorithmes cryptographiques sont présents dans une grande quantité de protocoles et d'outils de sécurité, dont TLS/SSL qui protège les flux à destination des sites web, SSH qui est utilisé pour l'administration des serveurs, ou les VPN permettant d'accéder à distance aux réseaux des entreprises. À titre d'illustration, des analystes estiment le nombre de sites web actifs dans le monde à 200 millions, dont environ 80 % sont sécurisés par TLS/SSL. L'utilisation de l'algorithme de Shor pour casser des clefs privées pourrait compromettre la sécurité des entreprises et des administrations, des citoyens et des consommateurs, des objets connectés et des terminaux, des moyens de paiement, des opérations de signature et d'archivage de documents, etc. La menace ne porte pas seulement sur les processus et les flux. Les données stockées sous forme chiffrée sont également concernées, ainsi que des données chiffrées qu'un attaquant aurait pu collecter en attendant de pouvoir les décrypter.

Une étude [2] de 2002 estime qu'il faudrait 2N+3 qubits pour exécuter l'algorithme de Shor sur un nombre de N bits, ce qui correspond à 4 099 qubits pour casser une clef RSA de 2 048 bits. Mais il s'agit de qubits logiques, sans erreurs. Or beaucoup plus de qubits physiques sont nécessaires pour réussir à faire fonctionner correctement les algorithmes quantiques. Différentes équipes de chercheurs proposent des approches pour casser une clef RSA de 2 048 bits et parviennent à un milliard de qubits physiques en 2012, 230 millions en 2017 et 170 millions en février 2019. En décembre 2019, une étude [3] aboutit à une estimation de 20 millions de qubits physiques et un temps d'exécution de l'algorithme de 8 heures. En 2021, un article [4] présente une architecture d'ordinateur quantique basée sur une structure de qubits en trois dimensions, qui permettrait de faire fonctionner un algorithme de Shor adapté pouvant casser une clef RSA de 2 048 bits en 177 jours avec 13 436 qubits physiques.

La marche à franchir est encore énorme entre la théorie et la pratique. En 2001, des chercheurs parviennent à factoriser le nombre 15 en mettant en œuvre l'algorithme de Shor sur un ordinateur quantique expérimental. En 2019, une équipe [5] employant un ordinateur quantique IBM de 16 qubits factorise les nombres 15 et 21 assez facilement. Pour le nombre 35, seuls 14 % des tentatives donnent le bon résultat, du fait de taux d'erreur importants lors de l'exécution du programme. En utilisant un autre algorithme nommé *Variational Quantum Factoring* sur un ordinateur quantique, des chercheurs [6] parviennent fin 2020 à factoriser le nombre 1 099 551 473 989. Fin 2022, une équipe [7] affirme avoir factorisé le nombre 261 980 999 226 229 avec un autre algorithme, nommé *Quantum Approximate Optimization Algorithm*, sur un ordinateur quantique de 10 qubits physiques. Les chercheurs indiquent qu'il faudrait, avec cette méthode, 372 qubits physiques pour casser une clef RSA de 2 048 bits, mais des spécialistes estiment qu'il n'est pas sûr que leur algorithme fonctionne correctement pour de telles tailles de clefs.

La question est de savoir quand les progrès des ordinateurs quantiques, la croissance du nombre de qubits disponibles et la réduction des taux d'erreur, voire la création de nouveaux algorithmes moins gourmands en qubits, permettront de casser une clef privée. Les estimations des analystes sont très larges, de dix à cinquante ans, avant que n'arrive le « Q-day », comme certains l'appellent. Les avancées des ordinateurs quantiques seront à court terme très visibles car les industriels rivaliseront dans les effets d'annonce. Mais, à plus long terme, les états les plus puissants seront sans doute moins diserts sur les capacités de leurs services de renseignement à construire ou acquérir de telles machines et sur le temps qui les sépare d'un ordinateur quantique capable de mettre en œuvre l'algorithme de Shor ou tout autre algorithme permettant de casser des clefs asymétriques.