

# L'information quantique : une révolution en devenir

## Introduction

**Au tout début de l'année 2021, le président Macron annonçait un plan de soutien de 1,8 milliard d'euros destiné aux technologies quantiques, il montrait par cet acte une volonté pour la France d'occuper une place importante dans ce domaine hautement stratégique. Ce qui est en jeu, c'est ce qu'il est convenu d'appeler la *deuxième révolution quantique* dont on commence à discerner le potentiel considérable d'applications.**

**Marc Leconte**

Membre émérite de la SEE

Les technologies quantiques ou plus exactement les applications de la physique quantique sont déjà anciennes si on y inclut les transistors et le laser qui ont en leur temps révolutionné la technologie. Cette *deuxième révolution quantique* intervenue il y a une quarantaine d'années avec l'information quantique est l'héritière à la fois des travaux de Schrödinger

et de ceux de Shannon. Ces technologies codent l'information numérique binaire avec des variables d'état spécifiques à la physique quantique. L'information quantique se décline en deux domaines *la cryptographie quantique et l'information quantique*. Le dossier qui suit s'intéresse à quelques aspects fondamentaux du développement actuel de l'information quantique.

### Origine de l'informatique quantique

Les supports théoriques de l'informatique quantique datent de presque un siècle. En effet la mécanique quantique connaît un premier aboutissement au congrès Solvay de 1927 qui voit s'affronter alors Albert Einstein et Niels Bohr autour du rapport à la réalité de

la nouvelle théorie. Einstein essaya jusqu'en 1935, par différentes expériences de pensée, de montrer que la mécanique quantique était incomplète. Parmi les expériences de pensée qu'il proposa, la plus célèbre a fait l'objet d'un article célèbre publié en 1935, co-écrit avec deux de ses collaborateurs, Nathan Rosen et Boris Podolski et connu sous l'acronyme d'article EPR. Or, dans cet article, Einstein décrivait une situation particulière dans laquelle les grandeurs physiques de deux particules quantiques ayant interagi, étant décrites par la mécanique quantique par une unique fonction d'onde, demeureraient corrélées après une mesure quelle que soit leur distance relative. Cette situation décrite par l'article EPR était explicitée peu de temps après par Shrödinger avec le terme d'*intrication*, traduction de l'anglais *entanglement*. L'intrication et le principe de superposition étaient alors considérés comme des propriétés théoriques mais qui n'avaient pas d'applications pratiques. Les choses ont changé à partir des années 60 quand l'expérience EPR à la suite d'un article de John Bell, a été réalisée à l'institut d'optique d'Orsay par Alain Aspect. le résultat de cette expérience conforta la mécanique quantique et montra que l'intrication avec la superposition pouvaient être mises en évidence dans des dispositifs expérimentaux.

### **Les idées de Feynman et l'algorithme de David Deutsch**

Richard Feynman, grand théoricien de l'électrodynamique quantique, déclarait lors d'une conférence au MIT en 1981 : « *La nature n'est pas classique, et si vous voulez faire une simulation de la nature, vous feriez mieux de la faire en mécanique quantique* ». Feynman posait avec cette proposition les fondements de ce qui allait devenir le calcul quantique, c'est à dire simuler et résoudre les équations de la physique quantique par des dispositifs expérimentaux.

**“L'idée d'utiliser des grandeurs quantiques comme les états à deux niveaux du spin des particules a alors fait son chemin et a été adoptée pour effectuer du calcul quantique. Ce système à deux niveaux a été appelé bit quantique et sa contraction en qubit est aujourd'hui universellement acceptée.”**

Les premières applications allaient suivre avec IBM qui publiait le premier protocole de cryptographie quantique en 1984. Le protocole BB84 était un système de distribution de clés quantiques dont la sécurité était garantie par les lois statistiques de la physique quantique. L'année suivante, David Deutsch, à l'université d'Oxford, établissait les principes d'un ordinateur quantique universel. David Deutsch s'était posé la question de savoir s'il existait une machine physique réalisée dans notre univers, utilisant de manière essentielle les principes de la mécanique quantique et qui serait apte à simuler n'importe quel phénomène s'y déroulant. Il répondait à cette question en expliquant que cette machine existait et que c'était l'ordinateur quantique. David Deutsch avait mis au point un algorithme quantique qui porte son nom (voir plus loin) qui montre de manière déterminante la supériorité de cet algorithme par rapport à une approche classique. L'idée d'utiliser des grandeurs quantiques comme les états à deux niveaux du spin des particules a alors fait son chemin et a été adoptée pour effectuer du calcul quantique. Ce système à deux niveaux a été appelé bit quantique et sa contraction en *qubit* est aujourd'hui universellement acceptée.

### **Des circuits logiques classiques au quantique**

Les circuits logiques qu'ils soient câblés ou programmés sont constitués par des portes logiques et c'est ce qui

constitue le cœur d'un ordinateur. Du point de vue théorique c'est Shannon qui a énoncé qu'il était possible de réaliser n'importe quelle fonction à l'aide de trois portes logiques OR, AND et NOT. Toutes les opérations de base d'un processeur sont réalisées en suivant ce théorème. En calcul quantique, quelques opérations logiques sont transposées et s'ajoutent à d'autres spécifiquement quantiques. La liste des opérateurs est représentée mathématiquement par des opérateurs linéaires et unitaires dans un espace de Hilbert. La linéarité est la caractéristique des mathématiques de la physique quantique ainsi que le caractère unitaire qui conserve la norme du vecteur d'état qui représente l'état du qubit. Ainsi un algorithme quantique à  $n$  qubits consiste, à partir des états de départ de l'algorithme, à manipuler l'état des qubits par des opérateurs linéaires et unitaires et à effectuer une mesure à la fin de l'algorithme.

### **Les opérations sur les qubits**

Nos ordinateurs de tous les jours effectuent des calculs et traitent les informations en utilisant le modèle de calcul standard (ou classique), qui remonte à Turing et Von Neumann . Dans ce modèle, toutes les informations sont réductibles en bits, qui peuvent prendre les valeurs de 0 ou 1. De plus, tous les traitements peuvent être effectués via de simples portes logiques (AND, OR, NOT, XOR, XNOR) agissant sur un ou deux bits à la fois, ou être entièrement ●●●

••• décrits par NAND (ou NOR). À tout moment de son calcul, l'état d'un ordinateur classique est entièrement déterminé par les états de tous ses bits.

La puissance de l'ordinateur quantique, quant à elle, réside dans son répertoire d'états beaucoup plus riche. Un ordinateur quantique a également des bits mais au lieu de 0 et 1, ses bits quantiques, ou qubits, peuvent représenter une combinaison 0, 1 ou linéaire des deux, ce qui est une propriété connue sous le nom de *superposition d'états*. Les outils logiques utilisés dans le calcul quantique ont été adaptés et pour certains transposés quand d'autres ont disparus. Le calcul quantique consiste à faire évoluer les qubits de leur état initial vers leur état final à l'aide de processus réversibles et la mesure finale, processus irréversible, est l'unique moyen d'extraire l'information utile après que les qubits ont atteint leur état final.

Les portes quantiques peuvent se décomposer en deux groupes, les portes à un qubit et les portes à deux (trois au maximum) qubits. L'expression générale d'un qubit s'écrit :

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  avec  $\alpha$  et  $\beta$  étant des nombres complexes.

$|0\rangle$  et  $|1\rangle$  sont les vecteurs de la base de mesure orthonormée écrits dans la notation de Dirac. La condition de normalisation impose  $|\alpha|^2 + |\beta|^2 = 1$ . Les opérations sur les qubits sont dites unitaires et réversibles. L'opération la plus simple d'un qubit et qui est l'équivalent d'une porte d'inversion classique est la porte X qu'il est possible de représenter par une matrice 2 x 2 qui échange les états  $|0\rangle$  et  $|1\rangle$  tel que  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

Elle est réversible car  $X^2 = 1$ . D'autres portes qui n'ont pas d'équivalence dans la logique classique s'écrivent :

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ et } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

**“ Par une utilisation judicieuse des portes quantiques, les algorithmes peuvent conduire à ce qui est appelé l'accélération quantique, ce qui signifie qu'un algorithme quantique est plus efficace ou plus rapide qu'un algorithme classique. ”**

La porte Z est un cas particulier de la porte de déphasage :

$$P(\gamma) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\gamma} \end{pmatrix}.$$

Les portes X, Y et Z ont pour représentation matricielle les matrices de Pauli qui sont utiles pour le calcul du spin (opérateur de spin).

L'ordinateur quantique tire parti de la superposition qui permet de nombreux états logiques ce qui est appelé parallélisme quantique ou parfois accélération quantique. La porte qui permet sur un qubit de réaliser une superposition des états de la base de calcul est la porte de Hadamard définie comme

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

Comme des coefficients diagonaux de la matrice ne sont pas nuls il est nécessaire pour conserver la norme de normaliser l'opération par  $\frac{1}{\sqrt{2}}$ . Cette dernière porte est aussi fondamentale qu'elle est simple, elle figure dans la quasi-totalité des algorithmes quantiques en superposant les états des qubits à l'entrée des calculs pour bénéficier de l'accélération quantique. Mais les calculs possibles seraient très limités si il n'existait que des portes à un qubit. Des portes à deux qubits ont donc été définies mais leur représentation matricielle est plus compliquée car les matrices 2 x 2 deviennent 4 x 4. La plus importante des portes à deux qubits est la porte cNOT (control NOT) qui se définit de deux manières :

$$C_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ et } C_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Il y a dans cette porte un qubit cible et un qubit de contrôle qui inverse ou non l'état du qubit cible. Il est possible d'utiliser une écriture plus compacte comme par exemple  $C_{10} |x\rangle |y\rangle = |x\rangle |x \oplus y\rangle$  expression dans laquelle le bit de contrôle x détermine l'état du bit y par un « ou exclusif ». L'association d'une porte de Hadamard à un qubit et d'une porte cNOT à deux qubits qui est une association à première vue relativement simple, a pour expression et conséquence l'intrication de deux qubits. En effet dans un système à deux qubits il se produit des corrélations et des interférences qui échappent au domaine classique.

## Les premiers algorithmes quantiques

### L'algorithme de David Deutsch

Par une utilisation judicieuse des portes quantiques, les algorithmes peuvent conduire à ce qui est appelé l'accélération quantique, ce qui signifie qu'un algorithme quantique est plus efficace ou plus rapide qu'un algorithme classique. L'un des tout premiers est celui proposé par David Deutsch en 1985 et qui utilise une fonction qu'on appelle *oracle*. Les calculs nécessitent le plus souvent l'évaluation de fonctions qui ne sont pas en général inversibles. La solution pour associer un opérateur unitaire à l'évaluation d'une fonction est d'introduire des qubits auxiliaires :

– un registre de données à n qubits qui contiendra la valeur de la variable ;

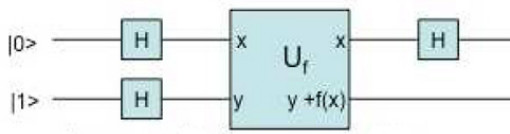


Figure 1 : Réalisation de l'algorithme de Deutsch.

– un registre de résultats de  $m$  qubits qui contiendra le résultat ;

– un opérateur unitaire agissant dans un espace des états à  $2^{m+n}$  dimensions.

L'opération s'écrit alors :

$$U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$$

Le problème posé par l'algorithme de Deutsch se formule de la façon suivante : soit  $f$  une fonction qui est soit constante, soit équilibrée, c'est à dire qu'elle vaut 0 dans la moitié des cas et 1 dans l'autre moitié. Pour déterminer si une fonction prise au hasard fait partie de l'une ou l'autre de ces catégories, il est clair qu'il faut calculer la fonction pour (au moins) deux valeurs différentes de la variable. David Deutsch a montré qu'en exploitant le parallélisme quantique on peut répondre au problème en une seule évaluation.

L'algorithme peut déterminer en une seule itération de la porte  $U_f$  si la fonction  $f(x)$  (voir figure 1) était équilibrée ou balancée alors que cela nécessite deux itérations dans un cas classique. Mais cette connaissance de cet aspect de la fonction s'effectue sans connaître les valeurs individuelles de la fonction. Cet algorithme se généralise à  $n$  qubits et porte le nom d'algorithme de Deutsch-Jozsa.

### L'algorithme de Grover

Cet algorithme proposé par Lev Grover en 1996 permet de trouver de manière efficace un élément particulier dans une base donnée non structurée. L'algorithme utilise un oracle qui grâce à la superposition s'applique à tous les éléments à tester. Grover a montré qu'il faut  $\sqrt{N}$  opérations alors qu'une version classique en nécessite  $N/2$ . Le gain

est significatif mais pas déterminant sauf pour des valeurs très élevées de  $N$ . C'est cet algorithme qui permet parfois aux médias d'affirmer que l'ordinateur classique peut casser les codes utilisés en cryptographie symétrique.

### L'algorithme de Peter Shor

En avril 1994 Peter Shor des Bell-Labs en s'appuyant sur les travaux de David Deutsch, Daniel Simon et Richard Jozsa, a élaboré un algorithme quantique de factorisation d'entiers de complexité polynomiale, donc beaucoup plus rapide que les meilleurs algorithmes classiques. Cet algorithme montrait d'emblée la fragilité du chiffrage RSA largement utilisé dans les communications et, pour cette raison, il a marqué le début d'une course vers le développement d'ordinateurs quantiques capables d'utiliser l'algorithme de Shor. Ce dernier (voir figure 2) est constitué de deux parties. La première consiste à calculer l'expression  $F(r) = a^r \bmod N$  (1). On rappelle que  $N$  dans le contexte RSA est le produit de deux nombres premiers que l'on recherche. Cette expression suppose le calcul d'une exponentiation modulaire, première étape de l'algorithme ; la deuxième étape consiste à déterminer la plus petite valeur de  $r$  pour laquelle l'expression modulaire (1) est vraie. Cette étape est effectuée par une transformée de Fourier quantique mise au point par Shor. La détermination de la complexité globale de l'algorithme est en  $O(N^3)$  ce qui reste de complexité polynomiale mais est plus rapide que n'importe quel algorithme de

factorisation classique. Cet algorithme est probabiliste, un nombre qui doit remplir certaines conditions est choisi, le calcul fournit alors un résultat qui peut être testé facilement et si le résultat n'est pas l'un des facteurs, il faut recommencer le calcul avec un autre nombre de départ.

### La suprématie quantique

En 2018, dans un article devenu une référence, John Preskill présentait le concept *Noisy Intermediate-Scale Quantum technology* (NISQ), technologie quantique à l'échelle intermédiaire bruitée. L'article développait l'argument que le développement des ordinateurs quantiques était appelé à passer par une étape intermédiaire dans laquelle un nombre significatif de qubits serait utilisé pour démontrer l'avantage du calcul quantique. C'est dans cet article qu'était avancée la notion de suprématie quantique d'un ordinateur qui serait caractérisé par sa capacité à effectuer une tâche impossible à effectuer par un ordinateur classique en un temps raisonnable. L'implémentation d'un algorithme de type Shor étant repoussée à moyen ou long terme. Les ordinateurs quantiques avec 50-100 qubits pourraient être capables d'effectuer des tâches qui dépassent les capacités des ordinateurs numériques classiques d'aujourd'hui, mais le bruit dans les portes limite la taille des circuits quantiques pouvant être exécutés de manière fiable. Les appareils NISQ dans cette vision nouvelle sont appelés à être des outils utiles pour explorer la physique quantique à  $N$  corps et pourront avoir d'autres applications utiles, mais l'ordinateur quantique ●●●

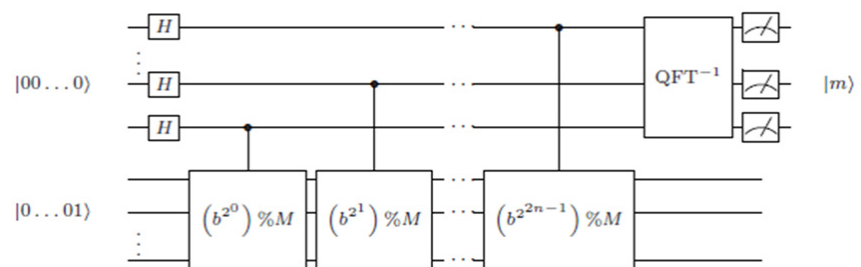


Figure 2 : Schéma de l'algorithme de Peter Shor. Les boîtes sur les lignes inférieures réalisent le calcul de l'exponentiation modulaire de la fonction (1) et les résultats sont injectés dans la transformée de Fourier quantique QFT. Il faut plusieurs milliers de qubits (logiques, voir plus loin) pour factoriser le  $N$  utilisé par le chiffrage RSA actuel.

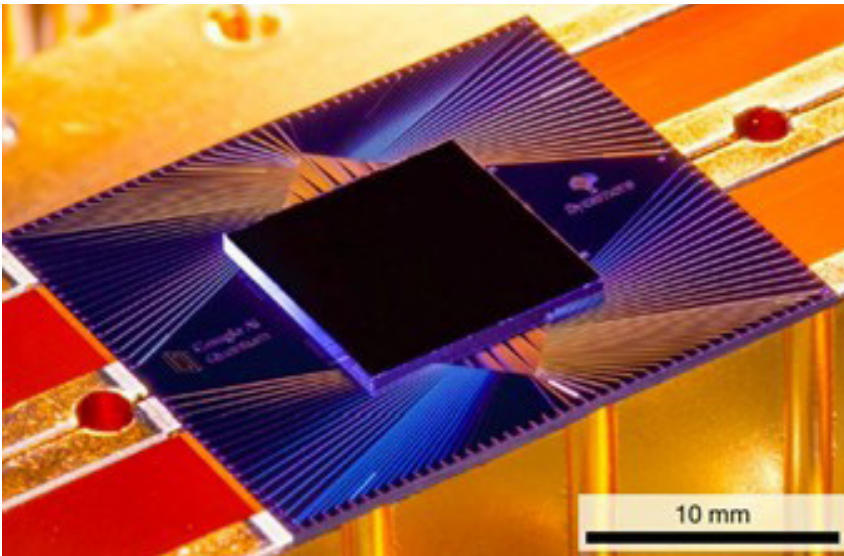


Figure 3 : Le processeur de suprématie quantique de Google dévoilé en 2019.

●●● à 100 qubits devrait être considéré comme une étape importante vers des technologies quantiques plus puissantes. Toujours dans ce cadre et de manière opportuniste et médiatique, Google a annoncé avoir atteint en 2019 la suprématie quantique avec son processeur Sycamore (figure 3).

## Les codes correcteurs

De nombreux acteurs du domaine ont longtemps pensé que le développement d'un ordinateur quantique serait impossible en raison de l'impossibilité de diminuer voire de supprimer le bruit et la décohérence des qubits. Mais ce sont les méthodes de *correction d'erreur quantique* qui ont permis de sauver les espoirs d'applications concrètes de l'ordinateur quantique. L'origine de ces algorithmes de correction remonte à Peter Shor qui a publié un article fondateur en 1995. La correction d'erreur est aujourd'hui largement utilisée mais a pour conséquence de déterminer deux types de qubits, les qubits logiques et les qubits physiques. Les qubits logiques sont ceux qui figurent dans les algorithmes quantiques et sont idéaux, les qubits physiques sont ceux des machines qui sont utilisés dans les calculs avec les systèmes de correction d'erreurs. Cela conduit à une multiplication du nombre de qubits nécessaires qui peut être très importante entre les deux types.

Pour une opération logique sur un qubit, il sera indispensable pour corriger les erreurs d'utiliser 10 voire beaucoup plus de qubits physiques. Cette démultiplication du nombre de qubits indispensables est l'un des aspects les plus importants aujourd'hui de l'informatique quantique.

## Le dossier quantique

Nous l'avons dit, la difficulté de développer un ordinateur ou un processeur quantique se heurte à des difficultés considérables qui sont liées pour l'essentiel à la technologie des qubits. Constatant ces difficultés les chercheurs ont défini des étapes à franchir plus réalistes que le simple fait de faire fonctionner l'algorithme de Shor de manière opérationnelle. C'est ainsi qu'a été proposé le NISQ (Cf. paragraphe précédent). **Xavier Geoffret**, responsable de l'expertise quantique de l'entreprise ATOS, décrit dans le premier article de ce dossier « L'algorithmie quantique à l'heure du NISQ ». L'implication de ce concept récent (Cf. paragraphe précédent) ouvre de nouvelles pistes dans les recherches d'algorithmes quantiques qui pourraient fonctionner sur des machines limitées en stabilité. L'article passe en revue les potentialités nouvelles et l'objectif de découvrir des algorithmes utiles et efficaces, en particulier dans les domaines d'optimisation et de *quantum machine learning*.

## L'auteur

**Marc Leconte** est ancien secrétaire du club RSSR de la SEE (radars, sonars et systèmes radioélectriques), membre du comité de rédaction de la REE, membre émérite SEE et médaillé Ampère. Au sein de Dassault Electronique, il a passé une quinzaine d'années à l'étude, au développement et aux essais en vol du radar RDI du Mirage 2000. Ensuite pendant trois ans, il a participé à l'étude d'un démonstrateur laser franco-britannique CLARA. A partir de 1995, il a élargi son activité aux domaines des études concurrentielles et stratégiques dans les domaines des radars aéroportés et de la guerre électronique. Il a exercé les mêmes activités dans la division aéronautique de Thales après la fusion de Dassault Electronique et de Thomson-CSF. A partir des années 90 et en parallèle, il s'est intéressé à l'histoire des sciences et des techniques et a publié plusieurs articles s'y rapportant.

Les qubits sont au cœur de l'ordinateur quantique et leur qualité détermine l'avenir du domaine. **Olivier Ezratty**, consultant spécialiste en informatique quantique, dresse dans l'article « les différents types de qubits », un état complet des différents type de qubits qui sont expérimentés aujourd'hui dans les centres de recherche étatiques mais aussi industriels. L'auteur explore les technologies mises en œuvre dans les recherches des meilleurs qubits car c'est là que se joue l'avenir de l'ordinateur quantique. Olivier Ezratty a entrepris depuis plusieurs années de faire comprendre l'informatique quantique grâce à un ebook et un blog dans lesquels tout ce qu'il faut savoir sur l'ordinateur quantique est exposé de manière claire.

## “Née avec ce qu’il est convenu d’appeler la deuxième révolution quantique, l’informatique quantique est devenue incontournable dans de nombreux domaines de la recherche et de la technologie.”

ATOS a fait le choix de ne pas développer d’ordinateur quantique mais de développer des simulateurs universels pour tous les types d’algorithme et de processeur. **Xavier Geoffret** dans l’article « De l’intérêt de la simulation quantique » illustre cette démarche d’ATOS. Il souligne la très grande variété des ordinateurs quantiques disponibles actuellement ou dans un proche avenir. Cette variété implique des jeux d’instructions différents pour la programmation. Xavier Geoffret explique donc qu’ATOS propose un simulateur universel capable de s’adapter à tout type d’ordinateur.

Les applications industrielles des algorithmes quantiques sont encore limitées. **Marc Porcheron**, Chef du projet « Informatique et technologies quantiques pour les métiers de l’énergie » à EDF R&D, présente dans un article au titre éponyme un certain nombre d’applications de l’informatique quantique dans la gestion de l’énergie au sens large. Cela concerne tout autant les problèmes potentiels liés à la gestion de la recharge des véhicules électriques quand leur nombre deviendra important que la sécurité des réseaux de gestion de la distribution et de la détection des défaillances. Une autre voie est également signalée qui est celle de l’intelligence artificielle avec des algorithmes quantiques adaptés au *machine learning*.

La société canadienne D\_Wave est l’un des acteurs les plus malaisés à classer dans le panel actuel des fabricants d’ordinateur quantique dont nos colonnes (REE 2016-1, 2018-5, 2021-3) ont évoqué à diverses reprises les avancées. En effet la qualité d’ordinateur quantique a bien souvent été refusée à leur production

commerciale de machine à qubits supra-conducteurs ce qui n’a pas empêché un certain succès auprès de grand comptes comme Google et de l’industrie d’armement des Etats-Unis tel que Lockheed. Le recuit quantique dont D-Wave s’est fait une spécialité est utilisé dans certaines applications spécifiques. **Cyrille Enderli** de Thales a ainsi développé une application d’optimisation de forme d’onde radar basée sur l’utilisation d’un processeur D-Wave utilisé en ligne qui fait l’objet du dernier article de ce dossier. Il explore ainsi dans quelle mesure les principes de calcul et de l’accélération peuvent se révéler plus efficaces que des circuits classiques dans des opérations d’optimisation spécifique, en l’occurrence ici des formes d’onde radar. C’est peut-être ce type d’applications qui à court et moyen terme fera le succès de l’informatique quantique.

### Conclusion

Née avec ce qu’il est convenu d’appeler la deuxième révolution quantique, l’informatique quantique est devenue incontournable dans de nombreux domaines de la recherche et de la technologie. De manière paradoxale, l’algorithme de Shor de facto-

risation avait lancé la course à l’ordinateur quantique mais devant les difficultés de développer une machine manipulant le très grand nombre de qubits nécessaires pour fragiliser le chiffrement RSA, les ambitions se sont orientées vers des objectifs plus limités en nombre de qubits mais qui obligent à intensifier les recherches d’algorithmes efficaces et utiles dans tous les domaines de l’ingénierie. En parallèle avec la technologie des qubits qui constitue un élément crucial, le développement de processeurs devrait profiter des progrès constants de la physique fondamentale de la matière ; il est probable que de nouvelles pistes pour des qubits seront trouvées comme par exemple l’émergence des qubits topologiques. ■

## Références

- PRESKILL, John Quantum computing in the NISQ era and beyond. *Quantum*, 2018, vol. 2, p. 79.
- DEUTSCH, David Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 1985, vol. 400, no 1818, p. 97-117.
- Feynman, R 1982 *Journal of theory physics*
- DEGIOVANNI, Pascal, PORTIER, Natacha, CABART, Clément, et al. *Physique quantique, information et calcul: des concepts aux applications*. EDP sciences, 2021.
- MERMIN, N. David *Calculs et algorithmes quantiques: méthodes et exemples*. EDP sciences, 2010.
- Olivier Ezratty : *Comprendre l’informatique quantique* ebook. <https://www.oezratty.net/wordpress/2020/comprendre-informatique-quantique-edition-2020/>
- <https://www.oezratty.net/wordpress/2021/understanding-quantum-technologies-2021/>

## Les articles

<b>L’algorithmie quantique à l’ère du NISQ</b> .....	p.54
<b>Les différents types de qubits pour les ordinateurs quantiques</b> .....	p.60
<b>De l’intérêt de la simulation d’ordinateurs quantiques</b> .....	p.68
<b>Informatique et technologies quantiques pour les métiers de l’énergie - Travaux en cours à EDF R&amp;D</b> .....	p.74
<b>Recuit quantique et optimisation de formes d’onde radar : un cas d’application du calcul quantique</b> .....	p.84