© Gorodenkoff / Shutterstock

Informatique et technologies quantiques pour les métiers de l'énergie

Travaux en cours à EDF R&D

L'Informatique quantique pourrait bouleverser dans les années à venir de nombreux domaines, dont celui des métiers de l'énergie… à condition que les incertitudes qui pèsent sur la réalisation de calculateurs de grande taille et robustes aux erreurs soient levées.

Marc Porcheron,
Christophe Domain,
Mohamed Hibti,
Paulin Jacquot,
Youssef Laarouchi,
Paul Lajoie-Mazenc,
Joseph Mikael,
Arthur Villard,
Ingénieurs-Chercheurs à EDF R&D

Introduction

L'informatique quantique nous fait trois promesses :

- Une augmentation de la puissance de calcul ;
- Une cybersécurité renforcée demain … et menacée aujourd'hui ;
- Des moyens de calcul moins énergivores.

Dans quelle mesure et à quelles échéances ces promesses seront-elles tenues ? Il est très difficile de le dire. Si nous pouvons déjà expérimenter certains algorithmes quantiques sur des calculateurs de quelques dizaines de qubits et sensibles au bruit quantique (*Noisy Intermediate Quantum Computers* (NISQC)), le passage à l'échelle vers des ordinateurs robustes aux erreurs et comportant un très grand nombre de qubits (*Large Scale Quantum Computers* (LSQC)) représente un défi scientifique et technologique considérable, à l'issue encore incertaine.

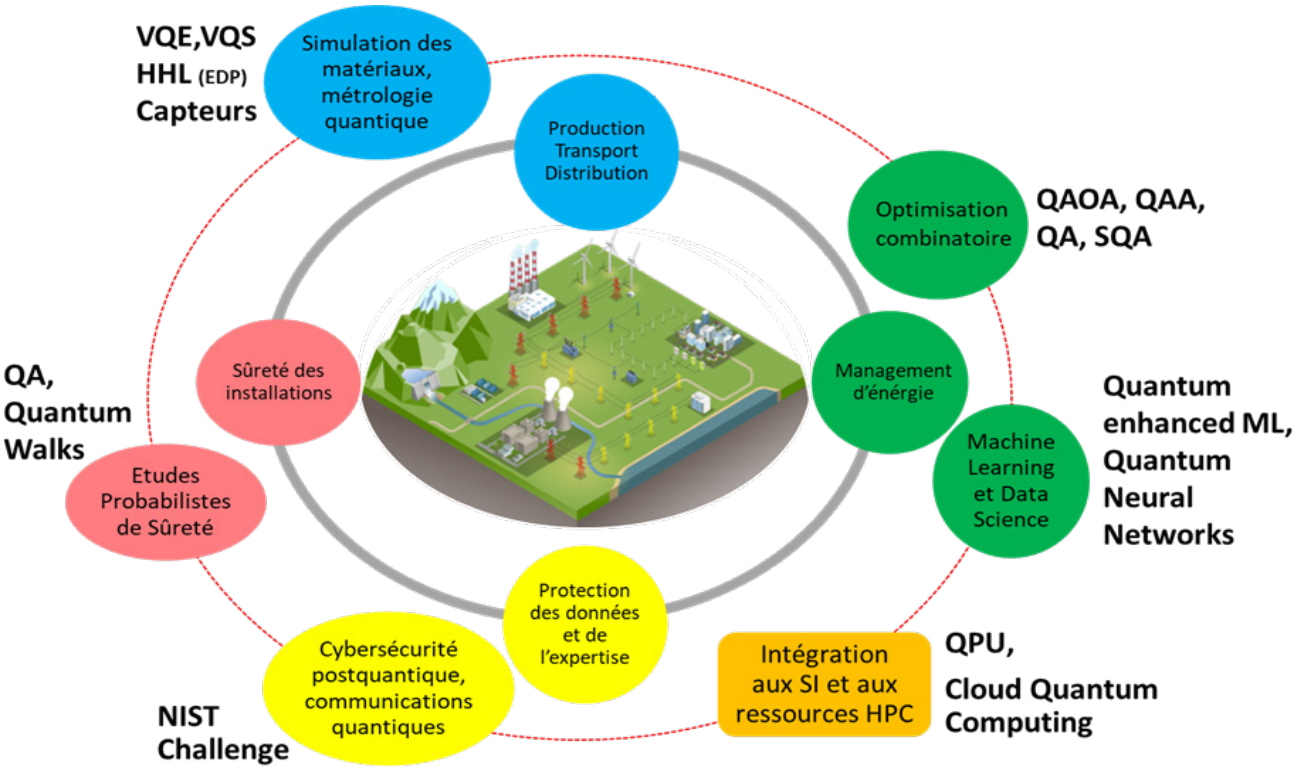


Figure 1 : Cas d'usages et technologies quantiques à l'étude à EDF R&D. QAOA : *Quantum Approximate Optimization Algorithm* ; QAA : *Quantum Adiabatic Algorithm* ; QA : *Quantum Annealing* ; SQA : *Simulated Quantum Annealing* ; VQE : *Variationnal Eigen Solver* ; VQS : *Variationnal Quantum Simulator* ; HHL : *Algorithm Harrow Hassidim Lloyd* ; QPU : *Quantum Processing Unit* ; NIST : *National Institute of Standards and Technology* (Organisme américain de normalisation dans le domaine de la cybersécurité).

Comme d'autres industriels, EDF s'intéresse aux technologies quantiques qui pourraient bouleverser nombre de ses métiers. La figure 1 synthétise les domaines et cas d'usage des technologies quantiques actuellement à l'étude à EDF R&D, qui seront présentées dans les sections suivantes.

Dans tous ces domaines, nous cherchons à évaluer de potentiels «avantages quantiques» en termes de performances ou de précision de nos codes, mais aussi en termes de performances énergétiques de nos moyens de calcul, un aspect rarement évoqué mais qui pourrait s'avérer déterminant pour l'avenir dans un monde où ordinateurs, centres de données, smartphones, tablettes et réseaux consomment déjà de l'ordre de 10 % de la consommation électrique mondiale [1].

Ces travaux sont menés en collaboration avec de nombreux partenaires académiques et industriels, dans le cadre de doctorats, de projets européens ou de projets s'inscrivant dans le Plan National Quantique récemment lancé en France.

Algorithmique quantique et optimisation combinatoire pour le management d'énergie

L'optimisation combinatoire est un des domaines les plus actifs de l'Informatique quantique, ceci pour une raison profonde : les problèmes de ce type ont d'innombrables applications et appartiennent pour la plupart à des classes de complexité algorithmique pour lesquelles on ne connaît pas d'algorithmes classiques de résolution exacts efficaces … et on soupçonne qu'il n'en existe pas [2].

L'enjeu qui consiste à résoudre efficacement ce type de problèmes est donc capital à la fois sur le plan pratique et sur le plan théorique, préciser l'apport du calcul quantique à cette classe de problèmes étant une question fondamentale encore ouverte. Le consensus actuel est que le calcul quantique ne permettra pas de résoudre en temps polynomial les instances les plus difficiles de ces problèmes. Des avantages quantiques significatifs sont en revanche espérés sur des problèmes particuliers, ou des instances particulières de ces problèmes [3].

On trouve ces problèmes à tous les niveaux des chaînes de production industrielles et de mise en œuvre de services, ●●●

1 Laure Cailloce « Numérique : le grand gâchis énergétique », Journal du CNRS (2018) https://lejournal.cnrs.fr/articles/numerique-le-grand-gachis-energetique. A. Auffèves, « Optimiser la consommation énergétique des calculateurs quantiques : un défi interdisciplinaire,» Reflets de la Physique, n° 169, pp. 16-20, 2021.

2 Il s'agit des classes NP, pour « Non-Déterministe Polynomial », et apparentées.

3 Deux algorithmes historiques ont apporté un début de réponse : celui de Peter Shor en 1994, à ce jour seul algorithme quantique présentant une accélération exponentielle sur un problème de la classe NP (la factorisation des entiers), et l'algorithme de Lov Grover en 1996 de recherche d'éléments dans un ensemble non-structuré, qui peut être utilisé pour fournir une accélération au plus quadratique sur ce type de problèmes.

mais ils apparaissent également dans quantité d'autres domaines où ils constituent souvent des goulots d'étranglement en termes de performances des codes de calcul.

En se limitant au domaine du management d'énergie tel que pratiqué par EDF, on peut citer les applications suivantes, de manière absolument non exhaustive :

- optimisation de l'équilibre offre-demande et des arrêts-démarrages des unités de production face au prix sur les marchés de l'énergie (*unit-commitment*) ;

- planification des arrêts pour rechargement des centrales nucléaires et des opérations de maintenance pendant ces arrêts ;

- optimisation des plans de rechargement du combustible en cœur, études probabilistes de sûreté ;

- optimisation des ressources pour les services clients (dimensionnement des centres d'appel …) ;

- planification des interventions sur le réseau de distribution (tournées de véhicules ...) ;

- optimisation de portefeuilles d'actifs de production sur les marchés de l'énergie ;

- recharge « intelligente » de véhicules électriques (*smart-charging*), dimensionnement et localisation des stations de recharge, etc.

Les méthodes quantiques pour l'optimisation combinatoire se déclinent essentiellement dans trois grandes familles d'algorithmes reposant sur les mêmes principes [1] [2] :

• **Le calcul adiabatique** (*Quantum Adiabatic Algorithm*, QAA) qui exploite la propriété d'un système quantique à rester dans un état fondamental d'énergie lors d'une évolution suffisamment lente de son hamiltonien ;

" L'enjeu est désormais de s'assurer du passage à l'échelle sur des instances de taille industrielle et d'estimer l'éventuel avantage quantique associé, ce qui suppose de disposer de machines quantiques plus robustes et plus puissantes en nombre de qubits qu'aujourd'hui. "

• **Le recuit quantique** (*Quantum Annealing* QA), restriction du calcul adiabatique à une classe particulière d'hamiltoniens et version quantique du recuit simulé classique, qui exploite l'effet tunnel pour sortir des optima locaux de la fonction à optimiser. Le recuit quantique peut être simulé classiquement, dans la limite d'une taille de problème compatible avec la puissance de calcul classique disponible (*Simulated Quantum Annealing* SQA) ;

• **L'algorithme quantique d'optimisation approchée** (*Quantum Approximate Optimization Algorithm*, QAOA), qui est une version discrétisée du processus analogique adiabatique, implémentable sur des circuits quantiques de faible profondeur, et donc particulièrement bien adaptée à la période NISQ actuelle.

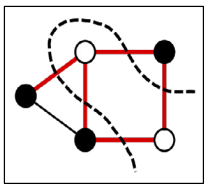
Dans toutes ces méthodes, la recherche de l'optimum du problème classique est rendue équivalente à celle de l'état d'énergie minimale (pour un problème de minimisation) d'un hamiltonien quantique bien choisi, appliqué à un ensemble de qubits représentant chacun une variable binaire du problème. L'avantage attendu repose sur la possibilité d'explorer efficacement et « en parallèle » l'espace exponentiel des solutions classiques au cours du processus de recherche de l'état fondamental de cet hamiltonien. Ces approches prometteuses présentent toutefois des difficultés importantes face à des problèmes de taille industrielle. Les hamiltoniens implémentables en pratique sont en effet le plus souvent des *modèles d'Ising*, c'est-à dire de systèmes de spins à deux états soumis à des interactions locales, et le problème doit être mis sous une forme adaptée, en l'occurrence quadratique en variables binaires et sans contraintes (*Quadratic Unconstrained Binary Optimisation problem*, QUBO). Cette transformation requiert l'ajout d'un très grand nombre de variables binaires auxiliaires à celles natives dans le problème, et en conséquence un très grand nombre de qubits est nécessaire pour implémenter concrètement ces méthodes sur des problèmes de grande taille.

EDF R&D teste actuellement activement ces approches sur des problèmes de management d'énergie, plus particulièrement dans le domaine de la recharge intelligente de véhicules électriques (*smart-charging*), domaine clé pour le développement de la mobilité électrique. La figure 2 ci-dessous illustre ces travaux, menés en partenariat avec le LORIA de l'Université de Lorraine, l'Institut d'Optique et sa spin off Pasqal, et Atos-Bull, dans le cadre des projets européens PASQUANS et NEASQC [4] .

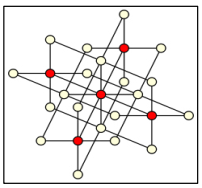
Les résultats obtenus sur de petites instances de ces problèmes sont très encourageants, les approches quantiques faisant au moins aussi bien que les meilleures approches classiques disponibles [3]. L'enjeu est désormais de s'assurer du passage à l'échelle sur des instances de taille industrielle et d'estimer l'éventuel avantage quantique associé, ce qui suppose de disposer de machines quantiques plus ro-

4 *Programmable Atomic Large-Scale Quantum Simulation* et *Next Applications of Quantum Computing*, respectivement.

- **Minimisation du temps total d'exécution d'un ensemble de charges priorisées**
- **Max-K-cut dans un graphe complet pondéré, NP-difficile.**



- **Minimisation du nombre de recouvrements d'intervalles de charge sous contrainte de groupe**
- **Stable Maximal (MIS)/Coloration d'un graphe d'union entre un graphe d'intervalles et un graphe cluster, NP-difficile**



- **Optimisation de la charge/décharge de véhicules électriques pour participation à la stabilité du réseau (*Vehicule-to-Grid V2G*)**
- **Très grand problème combinatoire faisant apparaitre des sous-problèmes NP-difficiles de plus court chemin sous contrainte de ressource dans des graphes**

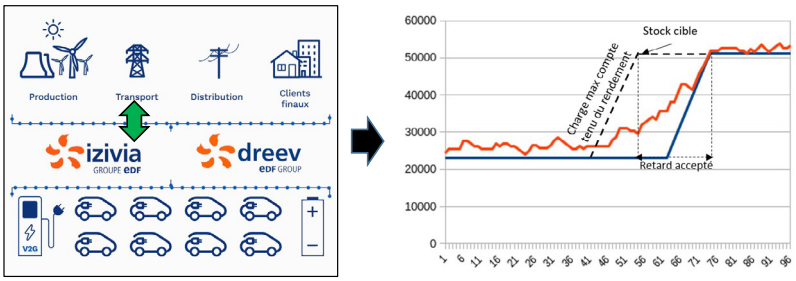


Figure 2 : Trois cas d'usage à l'étude dans le domaine du *smart-charging* de véhicules électriques.

bustes et plus puissantes en nombre de qubits qu'aujourd'hui.

Algorithmique quantique pour les études probabilistes de sûreté

Les études probabilistes de sûreté (EPS) sont des méthodes d'évaluation des risques fondées sur une investigation systématique, qualitative mais aussi quantitative, des scénarios accidentels d'un système. Elles sont aujourd'hui utilisées dans presque toutes les phases (design, construction, exploitation et démantèlement) de projets de systèmes industriels complexes et font maintenant partie de la régulation dans le domaine de la production nucléaire de l'électricité. On les retrouve dans plusieurs domaines industriels (pétrochimie, aviation et espace, transports ...).

La modélisation des EPS à EDF commence avec les *diagrammes de séquences* qui sont traduits en *arbres d'évènements*, dont les entêtes représentent des *missions système, facteur humain,* ou *contrôle commande*. Les diagrammes de séquences représentent les scénarios possibles à partir d'un évènement initiateur. Dans l'arbre d'évènements correspondant, les scénarios sont explicités en fonction du succès ou de l'échec des missions formant ainsi des branches composant les séquences allant de l'initiateur aux conséquences, dont celles indésirables qui nous intéressent.

L'évaluation quantitative des scénarios ou le calcul de métriques de risque (fréquence de chute d'avion, ou de fusion du cœur d'un réacteur nucléaire, ...) se heurtent à des problèmes d'explosion combinatoire et donc de complexité de calcul. Pour les modèles *statiques*, le problème est NP-Difficile et revient à trouver l'ensemble des combinaisons (quelques centaines de milliers ou quelques millions) d'évènements pouvant conduire à un évènement indésirable. Pour les modèles *dynamiques*, il est question de chercher l'ensemble des séquences allant d'un état de marche du système à un état inacceptable. C'est un problème d'*atteignabilité* qui est PSPACE-Complet.

Le calcul quantique donne l'espoir de voir se développer des méthodes tirant profit de la superposition et du parallélisme quantique pour parcourir les arbres et les graphes sous-jacents à ces modèles dans des temps raisonnables. Ces méthodes sont investiguées à EDF R&D en partenariat avec le LIPN de l'Université Paris Nord et Atos-Bull, dans le cadre du projet européens NEASQ.

Les *marches quantiques* semblent pertinentes grâce à leur capacité de traverser les graphes que l'on retrouve dans les modèles dynamiques et statiques, de façon parallèle en utilisant la superposition. Dans le cadre dynamique, elles constituent une piste particulièrement intéressante pour la recherche de séquences de l'espace d'état d'un système, impossible à traiter dans le cadre du calcul classique à cause de la difficulté de modélisation dans les différents formalismes utilisés et de la combinatoire exponentielle associée.

La combinaison d'*algorithmes de recherche* inspirés de celui de Lov Grover et d'*algorithmes de comptage* (*counting*) est ●●●

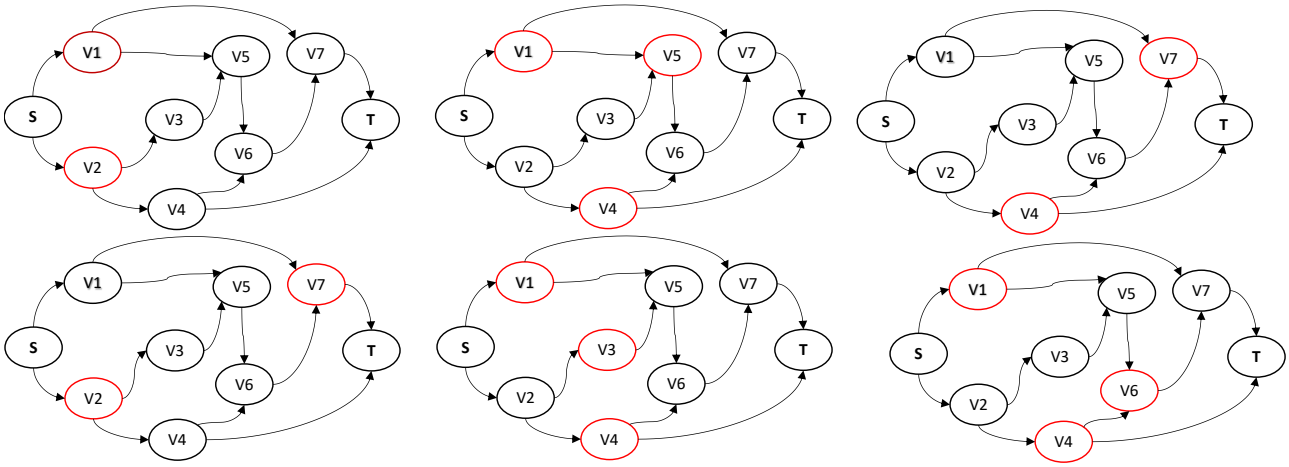


Figure 3 : Parcours d'un réseau *source-target* à la recherche de coupes minimales en utilisant des oracles de mouvement.

également étudiée. Ce type d'approches permet de résoudre, en utilisant des procédés d'*amplification de phase*, des problèmes de « satisfiabilité booléenne » tout en obtenant l'ensemble des coupes minimales [4]. En attendant l'arrivée d'ordinateurs quantiques avec un nombre de qubits important et une maîtrise du bruit, les algorithmes hybrides classiques/quantiques semblent permettre de travailler sur des instances de taille limitée, en utilisant une stratégie dite « *Divide & Quantum* » [5].

Les algorithmes de codage d'arbres de défaillances en utilisant des portes quantiques requièrent d'importantes ressources, même après une optimisation importante des circuits. En réduisant le problème statique d'une recherche de coupes ou d'impliquants premiers dans un arbre à un problème de recherche de « séparateurs de réseaux *source-target* », on peut envisager des algorithmes intéressants [6]. On utilise une stratégie de mouvements et de stockage à partir des états de marche (états initiaux) allant vers les états de panne, l'idée étant qu'à partir d'un état on passe « en même temps » dans les états suivants, grâce à la superposition. Ces transitions représentent les transitions de défaillance ou de réparation possibles à partir d'un état du système.

L'exemple suivant montre les étapes de recherche de coupes dans un graphe en utilisant des oracles de mouvements à partir des successeurs de la source, puis de proche en proche.

Sur la figure 4 on peut voir l'espace d'état d'un système de trois composants. On cherche à déterminer l'ensemble des séquences allant de l'état de marche initial |000> vers l'état de panne |111>. La figure 5 illustre la structure du circuit quantique utilisé. Après une préparation de superposition d'états par des Hadamards, on applique les différents oracles de mouvements. Le premier oracle en rouge permet de faire les transitions (|000> vers |100>, |010> et |001>), qui représentent les défaillances d'un des composants du système.

Simulation quantique des matériaux

La simulation de la structure électronique des matériaux et des molécules est une application de la mécanique quantique et un sujet d'application a priori naturel de l'ordinateur quantique, depuis les travaux de Richard Feynman.

Les calculs de structure électronique des matériaux sont basés sur la théorie

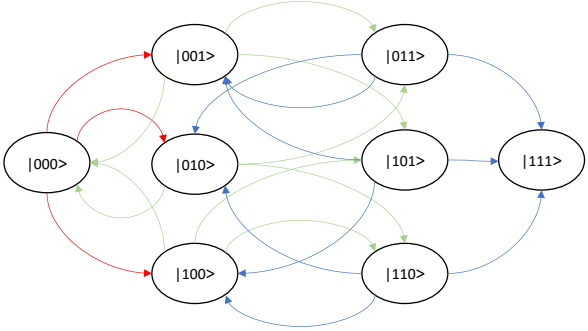


Figure 4 : Graphe de l'espace d'états.

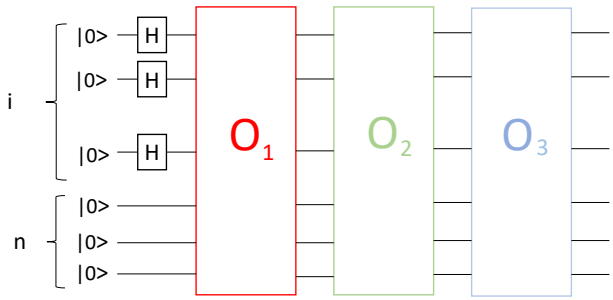


Figure 5 : Oracles de transition.

" A l'état de l'art, la simulation quantique des matériaux est limitée actuellement à des petits systèmes de quelques atomes essentiellement sous forme moléculaire."

de la fonctionnelle de la densité (DFT). Ils permettent aujourd'hui d'étudier avec précision les propriétés d'un grand nombre de matériaux, grâce au développement de fonctionnelles d'échange et corrélation GGA (*Generalized Gradient Approximation*), hybrides et avancées. Cependant, les matériaux avec une structure électronique fortement corrélée ne sont pas décrits (les semi-conducteurs des cellules photovoltaïques, les oxydes des électrodes de batteries ou des piles à combustible), tout comme les matériaux avec un magnétisme complexe comme les matériaux paramagnétiques et présentant de la frustration de spins (aciers austénitiques utilisés pour les internes de cuve des réacteurs des centrales nucléaires à eau pressurisée).

La prédiction du vieillissement de ces matériaux est un enjeu important pour EDF, en tant qu'exploitant des installations. Parmi, les méthodes d'étude du vieillissement, des travaux de modélisation basés sur les mécanismes élémentaires à l'échelle atomique sont menés, ces mécanismes étant caractérisés par des calculs de structure électronique nécessitant des moyens de calcul haute performance (HPC) importants. Les opportunités du calcul quantique pour améliorer la précision (et la rapidité) de ces calculs est donc un axe développé à EDF R&D.

A l'état de l'art, la simulation quantique des matériaux est limitée actuellement à des petits systèmes de quelques atomes essentiellement sous forme moléculaire.

Si la superposition d'un grand nombre d'états est une des forces de l'informatique quantique, le passage à de plus grands systèmes se trouve confronté à plusieurs verrous et plusieurs stratégies sont développées [7] [8] [9] dans la recherche académique et industrielle pour les lever :

• Réduire la taille du problème : ramener l'ensemble des interactions à une somme d'interactions plus simples (idéalement de paires), décomposer le système en plusieurs sous-systèmes ou ne traiter qu'une partie du système (i.e. quelques atomes / quelques électrons) par un calcul quantique et le reste par calcul classique – ce qui correspond à des méthodes hybrides ;

• Réduire le nombre d'opérations, ce qui revient à réduire la profondeur du calcul : écriture de l'hamiltonien, préparation des conditions initiales – état initial, les *ansatz* de résolution ;

• Réduire le nombre de qubits : ce qui peut être équivalent à simplifier le système global et à réduire le nombre d'atomes/électrons et leurs interactions à traiter ;

• Réduire le coût des corrections d'erreur, avec de nouveaux algorithmes.

EDF R&D, en collaboration avec l'Institut d'Optique, teste différentes approches (basées sur *Analog Quantum Simulation* AQS et *Variational Quantum Eigensolver algorithm* VQE) et différentes optimisations sur des petites molécules afin d'avoir la méthode et l'algorithme le plus frugal en termes de qubits et de nombres d'opérations ; ceci vise à la fois : (1) à étudier la faisabilité d'une mise en œuvre sur le système de qubits à ions piégés avec des atomes de Rydberg développés à l'Institut d'Optique, et (2) à pouvoir passer à un système plus grand, i.e. un matériau en volume.

Les auteurs

Marc Porcheron est ingénieur-chercheur sénior en Informatique Scientifique à EDF R&D, où il travaille depuis 1991, et dirige le projet « Informatique et technologies quantiques pour les métiers d'EDF » initié en 2020. Il est titulaire d'un doctorat en informatique de l'université Pierre et Marie Curie et d'une Habilitation à diriger des recherches. Ses recherches actuelles portent sur l'application des technologies quantiques à des problèmes d'optimisation dans le domaine du management de l'énergie.

Christophe Domain est diplômé de l'Ecole supérieure de physique et chimie industrielles de Paris, et docteur de l'université de Lille. Il est ingénieur-chercheur senior en modélisation multi-échelle en science des matériaux, vieillissement et matériaux innovants à EDF R&D qu'il a rejoint en 1997. Il est co-responsable du laboratoire commun EDF-CNRS « Etude et Modélisation des Mécanismes de Vieillissement des Matériaux », avec les universités de Lille et de Rouen. Il pilote les recherches sur la simulation quantique des matériaux et la métrologie quantique.

Quantum Machine Learning : perspectives pour l'algorithmique et pour l'industrie

Qu'il s'agisse de problèmes de classification, de contrôle optimal, de gestion d'actifs ou d'optimisation, le *Machine Learning* (ML) moderne a irrigué quasiment tous les domaines industriels. Parallèlement à cela, l'algorithmique quantique promet de changer la façon dont beaucoup d'algorithmes sont mis en œuvre. Il est donc naturel de questionner l'apport du quantique pour le ML d'autant que des résultats tendent à ●●●

montrer que certains algorithmes de ML quantiques sont robustes au bruit et à la décohérence qui caractérisent les machines quantiques de la génération actuelle dite « NISQ ». Le ML est ainsi considéré comme un bon candidat pour ces machines.

La mise en évidence d'algorithmes quantiques exponentiellement plus rapides que des algorithmes classiques pour certaines opérations d'algèbre linéaire a conduit la communauté du ML à s'interroger systématiquement sur toutes les méthodes de ML basées sur de l'algèbre linéaire et qui pourraient bénéficier d'une accélération quantique. Ces travaux ont donné naissance à la première génération d'algorithmes de ML à accélération quantique, basés sur l'algorithme *HHL*, d'une part, et l'analyse *en composantes principales quantiques*, d'autre part.

L'algorithme HHL [10] est un algorithme quantique pour *la résolution d'un système d'équations linéaires*, exponentiellement plus rapide que ses équivalents classiques sous certaines conditions. La résolution de tels systèmes est une brique de base du ML, mais aussi de beaucoup d'autres domaines de l'ingénierie. A EDF, de telles résolutions interviennent (via la résolution d'équations aux dérivées partielles) dans la simulation des structures ou celle des écoulements de fluides dans les unités de production, comme les barrages par exemple. Ces résolutions peuvent aussi intervenir dans des problèmes de contrôle, tels que la gestion d'actifs physiques.

La réduction de dimension via l'*analyse en composantes principales* (ACP) est l'autre brique de base de l'ingénieur, car elle représente une étape de prétraitement importante pour gagner en efficacité. Elle joue donc un rôle important dans l'apprentissage machine ainsi que dans l'exploration de données. L'ACP permet d'améliorer la qualité des modèles en concentrant l'effort sur les données d'intérêt. Il est difficile d'être exhaustif sur les applications de l'ACP dans une entreprise comme EDF. Elle est par exemple une pré-étape aux modélisations d'aléas de prix sur les marchés de l'énergie. Elle est aussi une pré-étape aux analyses économiques et autres analyses de risques. La version quantique de l'ACP (QPCA) propose une accélération exponentielle de l'ACP classique [11].

Ainsi, dotée de HHL et de la QPCA, la communauté a commencé à s'attaquer à des problèmes courants d'apprentissage machine. On obtient ainsi une accélération exponentielle sur les algorithmes de recommandation utilisés sur des plateformes comme Netflix ou Amazon ou par EDF pour faire de la complétion de données manquantes ou encore de l'identification de données aberrantes. On obtient aussi un gain exponentiel sur la *query complexity* des algorithmes de classifications (SVM) et de *K-Means clustering*, ce dernier algorithme permettant de classer une population en groupes. Ces étapes de classification sont utilisées par EDF notamment pour faire de la segmentation de clientèle ou de zones géographiques, étapes essentielles pour affiner les modèles de prévision de consommation au cœur d'enjeux importants pour le Groupe.

Le point de départ de tout algorithme de ML étant toujours un grand ensemble de données, la question de leur encodage sur une machine quantique est centrale. L'encodage est alors un arbitrage entre le nombre de qubits requis pour stocker N données, le nombre de portes nécessaires et la capacité de l'encodage à représenter les données dans un état dans lequel les calculs sont facilement réalisables et parallélisables.

L'efficacité remarquable des réseaux de neurones et du *deep learning* sur des problèmes variés comme la classification d'image, la génération de données ou l'aide à la décision, a amené la communauté à leur trouver des équivalents quantiques, recherche encouragée par le développement par Google de la version quantique de la bibliothèque de *Machine Learning*, TensorFlow. La voie n'est pourtant pas simple et beaucoup de défis restent à relever. Entre autres problèmes, les fonctions d'activation qui servent de briques de base aux réseaux de neurones sont non-linéaires et ne correspondent donc pas immédiatement à des circuits quantiques qui sont une succession d'opérateurs linéaires. Néanmoins, des techniques spécifiques, basées sur la mesure des systèmes quantiques, permettent de contourner ce problème. Des simili-réseaux de neurones basés sur des circuits quantiques paramétrés ont ainsi été appliqués avec succès sur des problématiques de classification, sur des bases de données de référence type MNIST (figure 6).

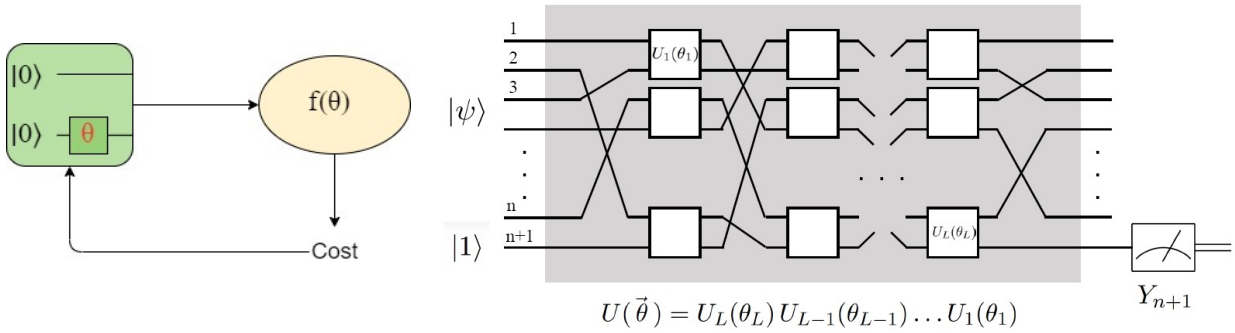


Figure 6 : Exemple d'un circuit quantique paramétré simple (à gauche) dont l'objectif est de minimiser f(θ) en modifiant θ. A droite : un circuit quantique paramétré où chaque carré représente une porte paramétrable.

Mais en dépit des avancées mentionnées ci-dessus, les réseaux de neurones sont aujourd'hui tellement rapides à entraîner et tellement peu sensibles à la dimension que l'on est en droit de se demander quel avantage quantique peut être attendu dans ce domaine. Un premier élément de réponse consiste à rappeler qu'une caractérisation de la suprématie quantique peut être liée à la *représentation des données*. Les tâches probabilistes impliquant l'échantillonnage ont en effet des chances de prouver l'avantage quantique à court terme. Le ML est justement un grand consommateur de méthodes d'échantillonnage. Elles interviennent notamment dans les méthodes génératives utilisées pour générer des images réalistes (*deep fakes*) ou des séries temporelles. Les générations de séries temporelles sont un sujet à enjeu pour EDF car elles permettent de générer des courbes de charges des clients fictifs (utiles pour l'anonymisation des données ou la *data augmentation*), des scénarios météo (utiles pour simuler des situations jamais vécues) ou des scénarios de prix. Un second argument est l'observation selon laquelle les circuits quantiques offrent une plus grande expressivité dans le sens où ils nécessitent moins de paramètres à caler pour le même résultat. Cela implique donc de fait des entraînements plus efficaces. Pour un groupe comme EDF, dépensant des dizaines de millions d'heures de temps CPU par mois pour entraîner des algorithmes de prévision ou de gestion optimale de parcs de centrales, cela présente un intérêt. Un dernier argument nous vient de l'article [11] dans lequel est construit un exemple de classification pour lequel une machine classique ne peut parvenir aux performances de la machine quantique.

Impact de l'informatique quantique sur la cybersécurité

La sécurité des algorithmes cryptographiques utilisés aujourd'hui repose sur la difficulté de la résolution de problèmes mathématiques sur les ordinateurs classiques. Deux problèmes principaux sont utilisés : *la factorisation de grands nombres*, sur laquelle repose la sécurité de l'algorithme RSA, ainsi que le problème du *logarithme discret*, utilisé par les algorithmes à base de courbes elliptiques. Il n'existe aujourd'hui pas d'algorithme exécutable sur nos ordinateurs classiques permettant de résoudre ces problèmes efficacement, c'est-à-dire en temps polynomial.

Cependant, en 1994, Peter Shor a proposé des algorithmes permettant la résolution de ces deux problèmes en temps polynomial, en exploitant les capacités d'un ordinateur quantique. Même s'il n'existe pas aujourd'hui, ou même à moyen terme, d'ordinateur quantique suffisamment puissant pour casser les algorithmes cryptographiques utilisés actuellement, il est nécessaire de concevoir dès maintenant de nouveaux algorithmes reposant sur des problèmes qui restent difficiles, même avec l'aide d'un ordinateur quantique.

En effet, le temps de développement d'algorithmes robustes et leur analyse n'est pas négligeable. En cryptographie, la confiance dans un algorithme repose dans les efforts qui ont été consacrés par la communauté pour essayer d'attaquer cet algorithme. En outre, le temps nécessaire pour migrer d'algorithmes classiques vers des algorithmes robustes, dits « post-quantiques », ne doit pas non plus être négligé. Finalement, la sécurité de certaines informations doit être assurée pendant de nombreuses années. ●●●

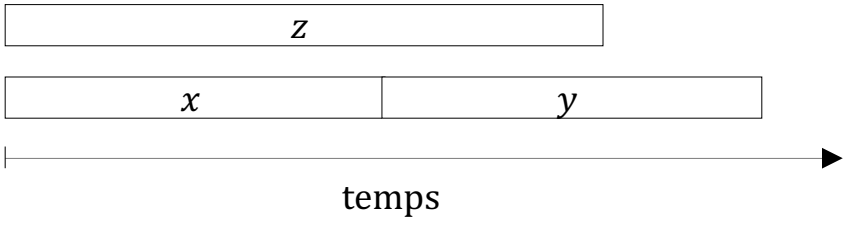


Figure 7 : Illustration du principe de Mosca : si le temps nécessaire pour construire un ordinateur quantique assez puissant (z) est inférieur au temps pour passer à des algorithmes post-quantiques (x) et à la durée pendant laquelle les informations doivent être sécurisées (y), les ordinateurs quantiques présentent un risque pour la sécurité.

Les auteurs

Mohamed Hibti est titulaire d'un doctorat en mathématiques et applications de l'université de Franche-Comté. Il a rejoint EDF R&D en 2001 pour travailler sur la sûreté nucléaire. Il est ingénieur-chercheur expert sur les problèmes de complexité algorithmique et travaille actuellement sur les outils avancés pour la modélisation des Etudes Probabilistes de Sûreté, et en particulier sur les apports potentiels de l'algorithmique quantique à ces études.

Paulin Jacquot est ingénieur-chercheur à EDF R&D depuis janvier 2021. Il est diplômé de l'Ecole polytechnique, et a effectué un doctorat en mathématiques appliqués à l'Ecole polytechnique puis un post-doctorat à Polytechnique Montréal. Ses thématiques de recherche principales sont l'optimisation, la théorie des jeux, les algorithmes distribués, l'informatique quantique, et leurs applications au système électrique et aux marchés de l'énergie.

Youssef Laarouchi est diplômé de L'école nationale supérieure d'électronique, informatique, et radiocommunications de Bordeaux. Il est titulaire d'un doctorat de l'université de Toulouse ainsi que d'une Habilitation à diriger les recherches. Il est actuellement chef d'un projet regroupant les activités de recherche en cybersécurité pour EDF et est co-responsable du laboratoire commun EDF R&D et Télécom-Paris « SEIDO, cybersécurité et internet des objets ».

Un attaquant pourrait enregistrer ces informations chiffrées dès aujourd'hui, pour les déchiffrer une fois qu'il aura accès à un ordinateur quantique. Ce raisonnement a été formalisé par Mosca [13] et est illustré sur la figure 7. Si « x+y> z », alors les ordinateurs quantiques présentent un risque pour nos systèmes : un attaquant pourra enregistrer des informations chiffrées avant que la migration ne soit effectuée, et les déchiffrer à l'aide d'un ordinateur quantique avant que ces informations ne perdent leur valeur.

Face à cette menace, le NIST, l'institut de standardisation américain, a lancé en 2016 un concours auprès de la communauté des cryptographes visant à identifier des algorithmes résistants à la menace d'un ordinateur quantique [14]. Concrètement, ce concours cherche à identifier plusieurs algorithmes dont la sécurité ne sera pas diminuée quand un ordinateur quantique suffisamment puissant verra le jour. La diversité algorithmique recherchée doit permettre, si un problème mathématique se révèle finalement plus faible qu'attendu, de disposer immédiatement d'alternatives sûres, contrairement à la situation actuelle où nous ne disposons pas d'alternatives prêtes à l'emploi et sûres pour remplacer RSA et les courbes elliptiques.

Si la Chine a organisé son propre concours pour identifier les algorithmes post-quantiques qu'elle utilisera, les agences de sécurité des systèmes d'information européennes, notamment l'ANSSI (France), le BSI (Allemagne) et le NCSC (Royaume-Uni), scrutent de près l'avancement de la compétition du NIST. En effet, ce dernier n'en est pas à son coup d'essai : il avait précédemment organisé les concours aboutissant aux standards AES, SHA1, SHA2 et SHA3, utilisés et reconnus aujourd'hui à l'échelle mondiale. Il faut également remarquer que l'Europe, et même la France, sont très bien représentés dans les soumissions du concours du NIST (voir encart).

Cependant, comme expliqué précédemment à travers le principe de Mosca, certaines données ont besoin dès aujourd'hui d'être protégées, sans pouvoir attendre les premiers résultats du concours.

Pour ce faire, une approche hybride, mêlant un algorithme classique et un nouvel algorithme post-quantique est possible. Cette hybridation permet de garantir :

- la sécurité des données contre la menace d'un ordinateur quantique grâce à l'utilisation de l'algorithme post-quantique ;

- la sécurité contre une défaillance nouvellement découverte du problème mathématique post-quantique grâce à l'utilisation de l'algorithme classique, dont la sécurité est éprouvée (face à un ordinateur classique).

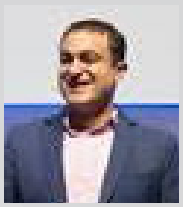
Ces constructions hybrides commencent à être recommandées par les agences européennes pour les données très sensibles devant dès aujourd'hui être protégées pour les dizaines d'années à venir. Pour les autres données, il reste recommandé d'attendre les résultats du concours avant de choisir les algorithmes utilisés.

Cependant, il est dès à présent possible de préparer cette migration vers le post-quantique : en 2020, l'ETSI (*European Telecommunication Standards Institute*) proposait des stratégies de migration, tandis que l'ANSSI (Agence nationale de sécurité des systèmes d'information) a commencé à communiquer en 2021.

Dans cette perspective, et au-delà de la veille active sur la compétition NIST et sur l'évolution des moyens de calcul quantiques, EDF envisage dès à présent plusieurs actions concrètes : identifier les données dont la sécurité devra être assurée à long terme ; prendre en compte « l'agilité cryptographique » en insérant des clauses spécifiques dans les cahiers des charges demandant aux fournisseurs de prévoir l'intégration d'algorithmes post-quantiques ; tester cette intégration sur des cas d'usage particuliers, en collaboration avec des sociétés spécialisées dans le développement de ces solutions. ■

Les auteurs

Paul Lajoie-Mazenc a reçu un diplôme d'ingénieur de Supélec en 2012, et a obtenu un doctorat en 2015 à l'Université de Rennes. Il a ensuite intégré EDF R&D en tant qu'ingénieur-chercheur en cybersécurité, où il s'est intéressé à la conception et à l'analyse de systèmes sécurisés, ainsi qu'aux techniques de protection de la vie privée.



Joseph Mikael est diplômé de l'université Paris Dauphine et a travaillé en tant qu'analyste quantitatif en salle de marché ainsi qu'en conseil, avant de rejoindre la R&D d'EDF en 2012 pour y travailler sur des problématiques de gestion des risques et de gestion actif-passif sur les marchés de l'énergie. Il est aujourd'hui ingénieur-chercheur expert sur ces thématiques et a piloté les activités de recherche sur l'application de techniques d'intelligence artificielle à ce domaine avant d'animer les travaux sur le Quantum Machine Learning.

Arthur Villard a obtenu un double diplôme d'ingénieur de l'Ecole polytechnique fédérale de Lausanne et de CentraleSupélec en 2018. Il a ensuite rejoint EDF R&D en tant qu'ingénieur-chercheur en cybersécurité. Il étudie les sujets innovants pour préparer le groupe EDF sur des thématiques telles que les nouvelles menaces, la sécurisation de l'Internet des Objets, les nouvelles méthodes d'authentification type FIDO2, ainsi que les risques et les opportunités liés à l'ordinateur quantique en cybersécurité.

Un concours plus européen qu'il n'y paraît

Le concours du NIST, bien qu'organisé par un organisme américain, a été conçu pour encourager les contributions venant du monde entier. L'Europe, et en particulier la France, sont très bien représentées : tous les finalistes participant au round 3 (7 finalistes + 8 alternatives) ont reçu au moins une contribution d'un laboratoire européen. De plus, parmi ces 15 algorithmes, 8 ont reçu une contribution d'un laboratoire français, démontrant ainsi le niveau d'expertise cryptographique présent en Europe et particulièrement en France.

Résumé

Promettant une puissance de calcul inégalable par des moyens classiques, l'informatique quantique pourrait bouleverser dans les années à venir de nombreux domaines, et EDF a naturellement entrepris d'en étudier l'impact sur ses métiers. Outre une veille active sur la cybersécurité post-quantique, les équipe d'EDF R&D mènent en collaboration avec de nombreux partenaires académiques et industriels des travaux approfondis sur les cas d'usage de cette technologie potentiellement disruptive. A cette étape, *la simulation des matériaux utilisés* dans les centrales, *l'optimisation* pour le management d'énergie, les *études probabilistes de sûreté*, et le *Machine Learning* ont été identifiés comme des champs d'application du « Quantum Computing » qui pourraient bénéficier d'un « avantage quantique » dans les années à venir… à condition que le défi à réaliser des calculateurs quantiques de grande taille et robustes aux erreurs soit relevé avec succès. ■

Abstract

Promising computing power unmatched by conventional means, quantum computing could revolutionize many fields in the years to come, and EDF has naturally undertaken to study its impact on its businesses. In addition to an active watch on post-quantum cybersecurity, EDF R&D teams are working in collaboration with numerous academic and industrial partners on in-depth studies on the use cases of this potentially disruptive technology. At this stage, the simulation of materials used in power plants, optimization for energy management, probabilistic safety studies, and Machine Learning have been identified as fields of application of «Quantum Computing» that could benefit from a «quantum advantage» in the years to come... provided that the challenge of realizing large-scale, error-robust quantum computers is successfully met. ■

Références

[1] E. Farhi, J. Goldstone et S. Gutmann, «Quantum computation by adiabatic evolution,» 2000. [En ligne]. Available: arXiv :quant-ph/0001106.

[2] E. Farhi, J. Goldstone et S. Gutmann, «A quantum approximate optimization algorithm,» 2014. [En ligne]. Available: arXiv:1411.4028v1.

[3] C. Dalyac, L. Henriet, E. Jeandel, W. Lechner, S. Perdrix, M. Porcheron et M. Veshchezerova, «Qualifying quantum approaches for hard industrial optimization problems. A case study in the field of smart-charging of electric vehicles,» . Europeean Physical Journal EPJ Quantum Technol., vol. 8, n° %112, 2021.

[4] G. M. Vinod et A. Shaji, «The integer case constraint satisfiability problem using Grover's algorithm,» arXiv, vol. 2106.09976, 2021.

[5] Araujo, I. F. a. Park, D. K. a. Petruccione, F. a. d. Silva et A. J, «A divide-and-conquer algorithm for quantum state preparation,» Scientific Reports, Vols. %1 sur %2https://doi.org/10.1038/s41598-021-85474-1, 2021.

[6] A. Zaiou, Y. Bennani, M. Hibti et B. Matei, «Algorithme quantique pour trouver les séparateurs d'un graphe orienté,» chez Conférence Internationale Francophone sur la Science des Données, Marseille, 2021.

[7] B. Bauer, S. Bravyi, M. Motta et G. Kin-Lic Chan, «Quantum algorithms for quantum chemistry and quantum matérials science,» Chemical Reviews, vol. 120, n° %122, pp. 12685-12717, 2020.

[8] S. McArdle, S. Endo, A. Aspuru-Guzik, S. Benjamin et X. Yuan, «Quantum computational chemistry,» Rev. Mod. Phys., vol. 92, p. 015003, 2020.

[9] Y. Cao, J. Romero, J. Olson, M. Degroote, P. Johnson, M. Kivlichan, T. Menke, B. Peropadre et N. Sawaya, «Quantum chemistry in the age of quantum computing,» Chemical reviews, vol. 119, n° %119, pp. 10856-10915, 2019.

[10] A. W. Harrow, A. Hassidim et S. Lloyd, «Quantum Algorithm for Linear Systems of Equations.,» Physical Review Letters, vol. 103, n° %115, 2009.

[11] L. Seth, M. Mohseni et P. Rebentrost, «Quantum Algorithms for Supervised et Unsupervised Machine Learning.,» 2013. [En ligne]. Available: arXiv Preprint arXiv:1307.0411..

[12] Y. Liu, A. Srinivasan et K. Temme, «A Rigorous and Robust Quantum Speed-up in Supervised Machine Learning.,» 2020. [En ligne]. Available: arXiv Preprint arXiv:2010.02174.

[13] M. Mosca, «Cybersecurity in an Era with Quantum Computers: Will We Be Ready?,» IEEE Security & Privacy, vol. 16, n° %15, pp. 38-41, 2018.

[14] NIST, «Post-Quantum Cryptography,» [En ligne]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography.