Cybersécurité et Calcul Quantique

Les risques de cybersécurité créés par l'irruption du calculateur quantique, ainsi que les différentes réponses.

À destination des spécialistes de cybersécurité qui …
… ont une culture scientifique, et des bases mathématiques minimales,
… ne sont pas experts en mécanique ni en calcul quantique,
… veulent comprendre comment fonctionne la mécanique et le calculateur quantique,
… (re)découvriront attaques quantique, cryptographie quantique et post-quantique.

Mémoire de CES « Architecture en cybersécurité »

Une formation certifiante et labellisée SecNumEdu FC par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), développée et délivrée par Telecom Évolution, Organisme de formation continue spécialisé dans le numérique, créé par les 3 écoles d'ingénieurs télécom, membres de l'Institut Mines Télécom : IMT Atlantique, Telecom SudParis et Telecom Paris.

Responsables Pédagogiques du CES : Yvon Kermarrec & Omessaad Hamdi

Année 2021/2022

Rédigé et soutenu par Fabien BATTINI, fabien@battini.bzh

Document version 0.25, 25 février 2022 ,
version soutenue le 3 mars 2022 devant le jury Telecom Evolution

Remerciements à :

ma tendre épouse, pour son soutien indéfectible,
mes enfants et petits-enfants, d'être la famille idéale,
Omessaad, pour avoir cru en mon projet,
Yvon, pour sa patience et ses conseils,
Guillaume, pour ses remarques toujours positives,
J.S.Bach, KJarrett et G.Verdi pour la musique,
Virgile, pour « Timeo Danaos et dona ferentes »

Introduction

La cybersécurité tient désormais une place prépondérante en informatique. Pour s'en convaincre, il suffit de lire la presse quotidienne nationale, qui se fait l'écho, de façon quotidienne, **d'attaques** sur des états (Ukraine, le ministère de la justice français…) des collectivités locales (Saint-Cloud), des ONG (croix rouge…), des grandes entreprises (Kaseya…) et des TPE, des particuliers. La presse liste aussi des **failles** de sécurité (Log4j…), et heureusement, quelques **succès** dans cette guerre cachée : Le démantèlement du groupe REvil, d'UniCC, l'augmentation de capital de Secure-IC… Aucun domaine informatique ne publie autant dans la presse grand-public !

Le bilan était déjà anxiogène. De surcroît, une autre menace plane, fondamentale : Les calculateurs quantiques sont-ils capables de « casser » les processus de sécurité actuel et mettre en danger tous les systèmes informatiques interconnectés ? Ce risque est-il inéluctable, va-t-il nous renvoyer à une ère pré-internet ? Disposons-nous de contre-mesures ?

Notre premier objectif est donc d'**appréhender les risques de cybersécurité générés par l'avancée des calculateurs quantiques**. Pour atteindre ce but, il semble indispensable de commencer par un long préliminaire sur les bases de la mécanique quantique, afin d'introduire les concepts qui font les spécificités du calculateur quantique.

Le second objectif est de **comprendre la stratégie française pour gérer ces risques**, et d'en déduire quelques actions qui semblent nécessaires pour le spécialiste de cybersécurité.

Il ne s'agit donc **pas** d'un mémoire de recherche, d'une thèse. L'idée n'est donc **pas** de référencer les travaux les plus récents, mais plutôt de donner une vision cohérente, utile pour la cybersécurité, et de permettre à chaque responsable de forger son idée et sa stratégie.

Ce mémoire s'adresse à des spécialistes de cybersécurité (RSSI, Analyste de sécurité, développeurs de systèmes sûrs…), ayant une culture scientifique – typiquement de niveau terminale -, mais pas nécessairement une compréhension récente de la mécanique quantique.

Le public visé est hétérogène vis-à-vis de la culture mathématique et de la volonté d'approfondissement des bases théoriques. Nous avons donc divisé ce document en 3 « couches » croissantes, indiquées par les conventions typographiques ci-dessous.

Cyber : Pour ceux qui ne sont intéressés que par les conséquences de la mécanique quantique en cybersécurité. Ils pourront sans dommage se passer de lire les autres niveaux.

> **MQ** : Pour ceux qui veulent comprendre les fondements de mécanique quantique qui sous-tendent les propriétés utilisées en cybersécurité, mais ne veulent pas plonger dans les mathématiques.
>
> > **Maths** : Pour ceux qui aimeraient avoir un embryon de compréhension des mathématiques sous-jacentes. On suppose ici une éducation mathématique typique de classe terminale, **on n'évoquera donc pas les développements qui nécessitent une culture de 3e année de licence** ou équivalent (calcul différentiel, intégrales, tenseurs, espaces de Hilbert…).

NB : toutes les citations sont en *« italique »*.

Table des matières

La ***partie 1 Rappels de mécanique quantique*** est une introduction rapide à mécanique quantique, qui met en évidence les points fondamentaux qui sont d'importance pour la cybersécurité. Quelques expériences-clefs, comme les inégalités de Bell, illustrent les notions.

La ***partie 2 Calcul Quantique*** est dédiée à la notion de qubit et aux premiers calculateurs Quantiques, à leur programmation, par exemple à travers l'algorithme de P.Shor, à l'état réel de l'industrie, et surtout explique les impacts potentiels sur la sécurité des systèmes informatiques.

La ***partie 3 Cybersécurité Quantique et post Quantique*** expose les différentes réponses de l'écosystème de la cybersécurité aux risques introduits par le calculateur quantique. *3.1 Cryptographie quantique* décrit une des applications particulières des calculs quantiques : la définition de nouveaux protocoles de sécurité. La sous-partie *3.2 Cryptographie Post Quantique* donne un aperçu des nouvelles méthodes de cryptographie qui résistent aux calculateurs quantiques. *3.3* fait le point sur la stratégie française.

La ***partie 4 Conclusions*** essaie de tirer quelques enseignements et introduit l'internet quantique, un concept qui émerge depuis quelques années.

La ***partie 5 Bibliographie*** liste les 187 références discutées dans ce document, avec leur URL.

1 Rappels de mécanique quantique

Cette partie **n'est pas** un cours de mécanique quantique, mais un rappel des principales propriétés de la mécanique quantique qui sont importants pour la sécurité des systèmes d'information.

Le lecteur qui voudrait un cours de mécanique quantique est plutôt invité à regarder le *[Chapitre 1.7 Pour approfondir]* qui propose une bibliographie spécifique, et le lecteur aguerri à cette discipline peut sauter toute cette partie 1, Rappels.

Comme indiqué dans le résumé, 3 niveaux de lecture sont proposés, il est conseillé de commencer par le niveau « Cyber » pour se familiariser avec les idées si particulières de la Mécanique Quantique, quitte à revenir plus tard sur les autres niveaux.

1.1 Une réalité

La mécanique quantique aura bientôt un siècle (ou un peu plus, suivant la date d'origine choisie).

La plupart des cours de mécanique quantique commencent par un rappel historique - voir par exemple *('Wikipedia: Histoire de la mécanique quantique', 2021)* - sur les raisons de son développement : la mécanique classique (newtonienne, électromagnétisme classique) ne permet pas de comprendre un certain nombre de phénomènes expérimentaux. Historiquement, ce sont le rayonnement du corps noir *('Wikipedia: Catastrophe ultraviolette', 2021)* puis l'effet photovoltaïque *('Wikipedia: Effet photoélectrique', 2021)* qui rendent nécessaire la refondation de la physique qui aboutira à la mécanique quantique.

La très grande légitimité de la mécanique quantique provient donc de sa capacité à expliquer des phénomènes, puis à en prédire des nouveaux : elle fonctionne !

La mécanique quantique apporte donc une compréhension de phénomènes microscopiques qui n'était pas accessible avant. Une de ses applications primordiales est la physique des semi-conducteurs, dont l'effet tunnel, sur laquelle reposent l'électronique et la réalisation matérielle de l'informatique.

Serge Haroche dans *(Haroche, 2016)* cite d'autres applications concrètes suivantes : les horloges atomiques, dont la base de temps est l'oscillation quantique des électrons dans les atomes, la supraconductivité, qui a permis le développement de

champs magnétiques intenses et donc de l'IRM. *('Wikipedia: Mécanique quantique', 2021) #Applications*, cite aussi le laser, le microscope électronique, la résonance magnétique nucléaire…

La mécanique quantique a aussi une grande pertinence aux très grandes échelles : Elle explique les raies spectrales des étoiles, les fluctuations primordiales issues du Big Bang…

Idée 1: Principe de réalité : La Mécanique Quantique, bien que difficile à appréhender et contre-intuitive, est validée.

Plus généralement, la mécanique quantique a été bâtie, entre autres, à partir d'expériences, que la mécanique classique ne peut pas expliquer, mais dont la mécanique quantique fournit une explication précise.

Dans la suite de ce chapitre, on illustre la Mécanique Quantique par quelques expériences qui sont des prétextes pour introduire les notions clefs qui aident à la compréhension des applications. Dans un premier temps, on survole l'expérience pour en exposer les conclusions importantes pour la cybersécurité, un second temps en détaille les aspects quantiques, et enfin un troisième temps propose des explications et démonstrations mathématiques, le lecteur pressé peut sauter ces deux derniers temps.

1.2 L'expérience des fentes de Young

L'expérience des fentes de Young met en évidence le comportement ondulatoire d'un phénomène physique en réalisant une interférence de l'onde avec elle-même. En passant par 2 fentes bien choisies, on peut observer l'interaction entre les parties d'ondes qui sont passées par chacune des fentes.

Cette expérience est réalisée classiquement sur une surface d'eau calme : On peut observer les vagues circulaires créées artificiellement par une pointe vibrante, puis utiliser un cache avec 2 trous pour mettre en évidence la figure d'interférence.

De façon plus étonnante, on peut aussi réaliser la même expérience avec de la lumière, des électrons, des atomes, des molécules…

L'interprétation de ces expériences introduit une première idée importante en Mécanique Quantique :

Idée 2 : Dualité Onde-Particule : « tous les objets physiques peuvent présenter parfois des propriétés d'ondes et parfois des propriétés de corpuscules. »
On peut donc associer une onde à chaque particule.

La mécanique quantique propose une interprétation de cette fonction d'onde, il faut pour cela introduire préalablement un nouveau concept :

Idée 3 : Superposition d'états : Un objet dont le comportement est décrit par la mécanique quantique peut être dans une superposition d'états potentiels. Le « choix » entre ces différents états n'est pas encore réalisé

Dans l'évolution d'un système quantique, la mesure est potentiellement l'évènement qui engendre des évolutions irréversibles, et donc de la libération d'entropie.

Dans notre exemple d'étude du spin de l'électron, l'état interne de l'électron peut être observé suivant 3 observables : La mesure du spin selon x, y et z. On pourrait aussi définir d'autres observables comme la mesure du spin selon la diagonale entre X et Z, par exemple. Tous ces observables peuvent être représentés par des matrices 2x2.

On pourrait démonter - ce qui est fait par *(Basdevant, Dalibard and Joffre, 2002), page 174 et suivantes* - que les mesures du spin de l'électron suivant les axes X, Y et Z peuvent être représentées par les matrices suivantes, dites Matrices de Pauli :

Formule 3 : Matrices de Pauli

$$MesureX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad MesureY = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad MesureZ = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

À chacune de ces matrices, on peut faire correspondre 2 états, dit ***états propres de la mesure***, dont la représentation n'est pas modifiée lorsqu'on le multiplie par la matrice. C'est-à-dire :

Formule 4 : État Propre

$$Mesure * |EtatPropre\rangle = |EtatPropre\rangle$$

En termes mathématiques, ce sont les « vecteurs propres » de la matrice. On les appellera $|X_+\rangle$ et $|X_-\rangle$ pour les vecteurs propres de la mesure suivant l'axe X, etc.

On pourra vérifier simplement que les valeurs suivantes sont correctes en multipliant la matrice de chacun des états par la mesure suivant le même axe :

Formule 5 : États Propres suivant X,Y,Z

$$|X_+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |X_-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$
$$|Y_+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \quad |Y_-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$$
$$|Z_+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |Z_-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Bra

À chaque ket $|\psi\rangle$, on peut associer un « Bra », qui sera noté $\langle\psi|$.
Lorsque $|\psi\rangle$ est une matrice colonne, par exemple $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ alors $\langle\psi|$ est une matrice ligne dont les coordonnées sont les conjugués des coordonnées de $|\psi\rangle$ soit $(\bar{\alpha}, \bar{\beta})$ [2] (rappelons que le conjugué de $z = x + iy$ avec x,y réels est $\bar{z} = x - iy$ et qu'il est souvent noté z^*)

Produit Scalaire $\langle Bra|Ket\rangle$

On définit un produit scalaire entre Bra et Ket, noté $\langle Bra|Ket\rangle$ qui forme le jeu de mots qui a donné leur nom au Bra et au Ket : Bra (c) ket = Bracket, soit crochet en anglais.

[2] Lorsque $|\psi\rangle$ est une fonction continue, alors $\langle\psi|$ est sa transformée de Fourier

De façon plus précise, 2 interprétations peuvent être proposées :

- **Variables locales « cachées » :** à un certain moment, par exemple lorsque les 2 électrons se sont séparés de leur atome originel, l'orientation du spin a été choisie pour chacun d'entre eux. Ce n'est donc pas la mesure par l'aimant qui a permis la détermination, mais cet instant originel. Cette valeur est ensuite transportée, de façon non observable (cachée) par l'électron, (dans sa fonction d'onde ?). Lorsque les mesures sont réalisées, il n'est donc pas nécessaire de communiquer quoi que ce soit.
  C'est l'intuition de EPR : Il faut trouver un complément à la mécanique quantique qui explique les variables locales cachées.
- **Non-localité :** Il est impossible de considérer les 2 électrons indépendamment, il faut considérer le système composé des 2 électrons ensemble.
  Ce système n'est donc pas localisé à 1 endroit. De la même façon que la fonction d'onde d'un seul photon passe par les 2 fentes de Young, la fonction d'onde du système intriqué est présente aux 2 localisations des 2 photons.

  Reste à déterminer comment la « coordination » entre A et B se passe, à quelle vitesse… et cela est encore du domaine de la recherche : il n'y a pas de consensus, voire (cf. *('Wikipedia: Inégalités de Bell', 2021) §6)* des interprétations divergentes.

Il faut aussi noter que dans l'hypothèse de non-localité, il n'y a pas de transport instantané d'information, contrairement à ce que laisserait penser l'intuition immédiate. Et c'est heureux, car, dans le cas contraire, la théorie de la relativité serait violée, car elle stipule qu'aucune information ne peut être transmise à une vitesse supérieure à celle de la lumière dans le vide.

En effet, la valeur de la mesure du spin de A est **aléatoire**, et ne constitue pas, en tant que tel, une information qui peut être utilisée : la mesure en B sera elle aussi aléatoire, (et synchronisée avec celle de A) on ne peut donc rien en déduire. Il faut pour cela d'autres éléments, qui respectent la relativité.

1.4.3 Inégalités de Bell

En 1964, (soit 29 ans après l'article EPR…) John Stewart Bell démontre le théorème qui porte son nom, et qui permet de trancher le paradoxe EPR en faveur de la non-localité.

Avant l'article de Bell, le débat EPR était essentiellement de nature philosophique. Bell propose un critère numérique à vérifier expérimentalement. Il faudra du temps pour que cela soit réalisé, mais toutes les expériences démontrent que les systèmes intriqués sont non-locaux, et que EPR avaient tort en recherchant une solution locale.

Les inégalités de Bell étant un des piliers de la mécanique quantique, le lecteur en trouvera des explications dans de très nombreux articles et cours de physique quantique. La plupart d'entre elles sont extrêmement complexes en matière de mathématique, ou alors éludent totalement les explications.

La suite de ce chapitre repose sur *(Quantum Walks, Bell, 2018)* qui est très didactique, et surtout (Bonsack, 1985) qui date de 1985, est particulièrement clair (j'en recommande la lecture), et est très souvent repris par des auteurs qui le résument souvent sans en conserver la clarté.

Bell considère un système « à variables locales cachées » et propose de la caractériser en faisant le strict minimum d'hypothèses. Il en tire une inégalité

2 Calcul Quantique

Ce chapitre est dédié aux premiers calculateurs quantiques, et leur impact sur la Cryptographie, donc la cybersécurité.

L'idée fondamentale du calculateur quantique est d'utiliser les propriétés de la mécanique quantique pour changer le paradigme de calcul. Intuitivement, si un calculateur peut calculer avec des états superposés, alors il devait être capable de calculer simultanément avec toutes valeurs possibles, et donc de rendre accessibles certains calculs qui sont réputés difficiles avec un calculateur classique.

2.1 Définitions

On s'intéresse ici au cœur de calcul (le CPU, le GPU, l'ALU pour le calculateur classique) du processeur d'un ordinateur, à la partie qui réalise les calculs. Tous les périphériques (mémoire de masse, entrées/sorties…) n'interviennent pas dans les calculs, et n'ont donc pas besoin d'être considérés.

Aujourd'hui, nous utilisons des ordinateurs « classiques », basés sur l'algèbre de Boole, en particulier à base de portes NAND ou NOR qui manipulent des mots composés de plusieurs (typiquement 1, 8, 32, 64) bits qui valent soit 1 soit 0. On sait depuis les travaux d'Alan Turing qu'un tel ordinateur est équivalent à une « machine abstraite de Turing » : pour un algorithme donné, les ordinateurs classiques ont une vitesse de traitement proportionnelle, sans changement notable dans la complexité calculatoire : passer à la nouvelle génération de CPU peut améliorer la vitesse d'un programme (typiquement d'un facteur 2 tous les 2 ans selon la loi de Moore), changer de type de RAM, de périphériques, utiliser des coprocesseurs MIMD, SIMD *(Colaïtis, Battini et al., 1995)* pourrait l'améliorer d'un facteur 4000, mais un algorithme dont la complexité est en n^2 restera en n^2…

NB : Un changement de langage de programmation peut parfois amener des changements de complexité, mais c'est parce qu'un nouvel algorithme a été rendu possible par un changement de sémantique du langage, par exemple en passant d'un langage qui n'autorise pas la récursivité à un autre qui l'autorise (mais on peut toujours dé-recursiver un algorithme à la main…) De telles améliorations sont rares avec les langages modernes.

Richard Feynman remarque rapidement que la simulation d'un système quantique par un ordinateur classique demande des ressources qui croissent exponentiellement avec la taille du problème étudié. On peut essayer de faire des hypothèses simplificatrices, elles sont soit trop fortes et conduisent à retomber dans une modélisation classique, soit trop faibles et ne permettent pas un gain de complexité.

Benjamin Lévi, dans sa thèse de 2004 *(Benjamin Lévi., 2004)*, donne une introduction compréhensible de ces phénomènes, et nous conclurons avec lui *« Pour simuler efficacement un système quantique, il faut donc faire appel à un ordinateur qui fonctionne lui aussi selon les lois de la mécanique quantique. »*

Idée 20 : Calculateur quantique. On appellera « calculateur quantique » un calculateur qui exploite les lois de la mécanique quantique et permet au programmeur d'en tirer parti.

Le terme « suprématie » est très frappant, et donc l'objet de nombreuses communications qui peuvent tenir plus du marketing que de la publication scientifique, on le retrouve donc régulièrement dans les médias grand-public, en particulier à l'occasion de **la controverse Google/IBM de 2020**.

À l'origine, -Octobre 2019- Google annonce avoir atteint la suprématie quantique *(Le Monde.fr, 2020)* grâce à une puce Sycamore à 53 qubits. Mais Cette communication est violemment contestée par IBM. L'article que Frandroid a consacré à cette controverse *(Castro, 2019)* a l'intérêt d'être claire et de pointer sur les articles d'origine.

En résumé, IBM expose *(On "Quantum Supremacy", 2019)*, que Google compare son programme quantique avec un programme classique de mauvaise qualité, alors qu'IBM dispose de techniques de simulation bien plus complètes, en particulier qui utilisent des disques durs pour le stockage de données (au lieu de RAM), et des techniques d'optimisation de l'accès mémoire, qui permettent de réaliser la simulation en quelques jours. Pour IBM, le gain proclamé par Google est donc non avenu.

La course est cependant bien lancée, et les communications se succèdent.

2.3.2 Les applications

La première application du calculateur quantique est, historiquement, la simulation de systèmes quantiques. On retrouve d'ailleurs ici une des caractéristiques uniques de l'informatique : la capacité de « bootstrap » au sens propre, c'est-à-dire d'utiliser les machines de génération N pour concevoir les machines de génération N+1. Et c'est cela qui explique le développement fulgurant de cette industrie. Le même phénomène se reproduira-t-il pour le calculateur quantique ?

Le calculateur quantique se prête bien aux problèmes de combinatoire qui font intervenir un « petit » nombre N de données, mais où l'algorithmie classique est une fonction exponentielle de N, et où la capacité de calcul simultané du calculateur quantique sera utile. Inversement, les calculs séquentiels, ou portant sur un grand nombre de données, ont peu d'intérêt.

Au-delà de la simulation des processus quantiques, les applications suivantes des calculateurs quantiques sont régulièrement citées *(Qu'est-ce que l'informatique quantique ?, Permanent) (Microsoft Quantum overview, 2022),* et avec force détails dans *(Quantum computing use cases--what you need to know | McKinsey, 2021)* :

- La simulation de molécules complexes, en particulier pour la simulation de médicaments
- L'optimisation chimique, en particulier des catalyseurs
- La recherche opérationnelle, qui est bien souvent un problème d'optimisation de grande taille, dont l'exploration combinatoire est impossible par un ordinateur classique
- La simulation de systèmes complexes, comme les batteries de nouvelle génération, l'optimisation du transport de l'énergie, en particulier en utilisant la simulation de Monte-Carlo …
- L'intelligence artificielle, ou plutôt le deep learning, qui en est uniquement l'une des instances, en particulier pour l'analyse d'images médicales.
- L'analyse et l'optimisation financière.

2.5.3 Amazon

L'offre publique d'Amazon est portée par AWS, et donc, sans surprise, est une plateforme disponible dans le cloud *(Service d'informatique quantique | Amazon Braket | Amazon Web Services, 2022)*. L'accent est mis sur la disponibilité du service, sa tarification à l'usage, et la disponibilité d'une offre de 1 heure de simulation par mois (pendant la 1ere année). Quelques applications industrielles sont présentées rapidement.

Amazon met à disposition des plateformes matérielles qui permettent d'expérimenter 3 types de calculateurs quantiques, basés sur des pièges à ions de **IonQ**, des super-conducteurs de chez **Rigetti** et des dispositifs de recuit en provenance de **Dwave**.

2.5.4 IBM

Le site public d'IBM pour le calcul quantique est *(IBM Quantum Computing, 2022)*. Conscient des difficultés du domaine, IBM fait d'abord la promotion des applications avec des grands partenaires (Mercedes, Exxon Mobile, CERN), et collabore étroitement avec les gouvernements Européens *(Yahoo! news, 2021)*

La page racine du site IBM consacré à la vulgarisation de l'informatique quantique est disponible en Français *(Qu'est-ce que l'informatique quantique ?, Permanent),*

IBM décline sa gamme de solutions en 3 catégories : Pour le business, les chercheurs, les programmeurs.

IBM a annoncé le 16 Novembre 2021 une puce '**Eagle**', à **127 qubits**. *(IBM Quantum breaks the 100-qubit processor barrier, 2021)*, et prévoit *(IBM's roadmap for scaling quantum technology, 2021)* une puce à 1000 qubits pour fin 2023 !

Les documents plus techniques sont disponibles en anglais uniquement *(F. C. IBM Quantum Computing, 2022)*

Le calculateur d'IBM qui comporte des processeurs quantiques est appelé « **Quantum System One** », *(IBM Quantum System One, 2018)*. Son cœur de calcul quantique est pour l'instant Falcon, et il pourra être upgradé avec Eagle qui vient d'être annoncé. Ce calculateur est disponible en version commerciale pour les entreprises qui ont besoin de disposer de leur propre calculateur quantique. La technologie est basée sur la supraconduction à très basse température, le calculateur est donc cryogénisé et doit être placé dans des conditions immunes aux vibrations et autres perturbations.

La programmation se fait avec l'outil Qiskit *(Qiskit, 2022)*, qui est un SDK open-source, il offre 3 vues du système : qubits, circuits et applications.

Le blog d'IBM *(IBM Research Blog | IBM Research, 2021)* est une bonne façon de rester en contact avec les avancées de cet acteur majeur.

2.5.5 Alibaba et Baidu

Alibaba a choisi d'investir dans sa propre technologie de calculateurs quantiques. **NextPlatform** (qui est aussi un site de référence utile) lui consacre un article *(Hemsoth, 2021)*. Le processeur quantique dispose de 11 qubits, et le simulateur permet d'expérimenter virtuellement avec un cœur à 64 qubits.

Il ne faut pas non plus mésestimer le risque qu'une attaque ne soit pas violente et visible, mais cachée et insidieuse, à la façon des « Advanced Persistent Threats ». La génération de quelques transactions bancaires pourrait être rémunératrice, la déstabilisation lente d'un état est une opportunité, voir à ce sujet les attaques contre l'Ukraine en janvier 2022 *(Le Monde, 2022)*.

2.6.4 Horizon du risque

(NAP, 2019) affirme:

> **Idée 39 : RSA, Un risque à horizon lointain.** "Key Finding 1 (2019) : Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

(NAP, 2019) indique aussi p. 97 que, **pour casser une clef RSA de 2014 bits, il faudrait disposer d'un calculateur qui a autour de 2300 ([7]) qubits logiques**. C'est cette conclusion qui a poussé le NIST à déclencher dès 2016 la recherche d'un remplacement pour la cryptographie asymétrique classique (que nous verrons dans la prochaine partie).

P. 98, *(NAP, 2019)* propose la table suivante, qui résume le consensus de la littérature en 2018 :

Crypto système	Catégorie	Taille des clefs	Algo quantique	Qubits logiques	Qubits physiques	Temps nécessaire	Remplacement
AES-GCM	Symétrique	128 192 256	Grover	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years	inutile
RSA	Asymétrique	1024 2048 4096	Shor	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours	NIST PQC
ECC Discrete-log	Asymétrique	256 384 521	Shor	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours	NIST PQC
SHA256	Bitcoin mining	P = 72	Grover	2,403	2.23×10^6	1.8×10^4 years	inutile
PBKDF2 10,000 iter	Password hashing	P = 66	Grover	2,403	2.23×10^6	2.3×10^7 years	Change to « no password »

Figure 10 : Tailles de clef et risque quantique

Ce que l'on résumera ainsi :

[7] On notera que ceci est incohérent avec la table juste en dessous, pourtant issue du même document.

L'ENISA a publié en mai 2021 une revue complète de l'état des menaces et des propositions faites au NIST *(Post-Quantum Cryptography: Current state and quantum mitigation, 2021).*

On en tire le résumé suivant :

- L'objectif est de définir des algorithmes qui résisteront aux calculateurs quantiques futurs, car les actuels ne permettent pas encore d'attaquer les algorithmes classiques
- En ce qui concerne la cryptographie symétrique, une augmentation de la taille des clefs permet de garantir l'immunité aux attaques quantiques, avec un coût calculatoire et de stockage qui n'est pas rédhibitoire.
- Le processus est public, et les propositions des différentes équipes est soumis à l'analyse de la communauté scientifique.
- 2 problèmes distincts sont étudiés : Le chiffrement d'un document, qui permet d'en garantir la confidentialité, et la signature, qui permet d'en garantir l'intégrité.
- Le processus en est à la 3e itération, ont été choisis 7 finalistes (4 chiffrements et 3 signatures) et 8 technologies alternatives, au cas où les finalistes soient tous en échec.

Les finalistes utilisent 3 familles différentes de problèmes difficiles :

Schéma	Enc/sign	Famille	Problème
Classic McEliece	Chiffrement	Code-Based	Decoding random binary Goppa codes
Crytals-Kyber	Chiffrement	Réseaux Euclidiens	Cyclotomic Module-LWE
NTRU	Chiffrement	Réseaux Euclidiens	Cyclotomic NTRU Problem
Saber	Chiffrement	Réseaux Euclidiens	Cyclotomic Module-LWR
Crystals-Dilithium	Signature	Réseaux Euclidiens	Cyclotomic Module-LWE and Module-SIS
Falcon	Signature	Réseaux Euclidiens	Cyclotomic Ring-SIS
Rainbow	Signature	Multi-variés	Oil-and-Vinegar Trapdoor

Cependant, le compte-rendu de la 3e conférence NIST *(Dustin Moody, 2021)* indique que les cryptanalyses conduites pendant la 3e phase ont montré des « problèmes » avec Rainbow, qui sera sans doute abandonné, alors que Sphincs+, qui n'était pas initialement finaliste, est très avancé et très sûr.

Idée 47 : État de la standardisation de la PQC par le NIST, janvier 2022.
La 4e phase de la compétition était censée démarrer fin 2021, elle ne devrait donc pas tarder (8) à être annoncée, sa durée devrait être de 12-18 mois, les drafts publics pour commentaire devraient arriver en 2022-2023, et le standard en 2024.

Il est vraisemblable que plusieurs schémas seront standardisés.

Les critères de décision sont :

- **Sécurité :** Les niveaux de sécurité, leur explication par des preuves, les attaques, l'analyse de la complexité classique et quantique.

[8] Écrit en janvier 2022

3.4 La stratégie Française de Calcul Quantique

3.4.1 Le rapport Forteza

Le document fondateur de la stratégie de l'état français en matière de calcul quantique est le rapport Forteza *(P.FORTEZA, 2020)*. Il conclut une mission parlementaire qui s'est déroulée du 15 avril au 3 octobre 2019. Les principales motivations sont la croissance économique et la souveraineté technologique avec en particulier le risque cybersécurité induit par l'émergence des calculateurs quantiques.

Le rapport propose 5 ambitions :

- Devenir l'un des leaders mondiaux en matière de calculateurs quantiques tolérants aux défauts (LSQ)
- Devenir le leader européen en matière de calculateurs quantiques bruités de taille intermédiaire (NISQ)
- Devenir l'un des leaders mondiaux en matière de logiciels métiers
- Jouir d'une large autonomie industrielle sur les technologies habilitantes, en particulier les capteurs à base des impuretés dans le diamant

Idée 50 : Le 5eme axe stratégique du rapport Forteza est « Maintenir une indépendance stratégique sur les technologies de cryptographie »

Pour arriver à cet objectif, le rapport recommande d'une part un soutien au développement de la technologie, des usages, et d'autre part des règles de gouvernance qui facilitent l'innovation. Il fait aussi 37 propositions, dont on cite ici celles qui sont directement relatives à la cybersécurité :

Idée 51 : Le rapport Forteza fait 5 propositions d'investissement en cybersécurité lié au calcul quantique

Proposition 28 : Inclure 6 ECTS d'algorithmie quantique dans les vingt principaux cycles d'ingénieurs en informatique et 6 ECTS de cryptographie post-quantique et quantique dans les masters de cryptographie

Proposition 4 : Déployer une plateforme de test pour différents dispositifs de communications quantiques.

Proposition 19 : Soutenir, à travers les concours i-Nov et les dispositifs de soutien et d'accélération de l'innovation des ministères concernés, le développement, avant 2022, d'une offre compétitive de cryptographie post-quantique pour systèmes à ressources de calcul limitées.

Proposition 20 : Élaborer une stratégie d'évaluation des systèmes QKD s'appuyant sur le schéma de certification français et européen

Proposition 21 : Soutenir, à travers les AAPR de l'axe « Technologies Quantiques » de l'ANR, une action de recherche relative à la maturation de la technologie QKD (systèmes à variables continues et à variables discrètes, relais quantiques, liens satellite, etc.) impliquant les experts des communications quantiques, les experts de la cybersécurité et les équipementiers télécoms.

Cette révolution est analogue à celles dues à l'électricité, l'énergie nucléaire, internet, les réseaux sociaux. Un seul calculateur quantique peut donner un avantage décisif à son propriétaire, par exemple en permettant de pénétrer les communications sécurisées, le réseau bancaire… Tout **état** stratège, tout **leader industriel ou académique** dans un domaine impacté se doit d'investir dans ce domaine.

En revanche, les verrous technologiques sont encore très nombreux et fondamentaux. Il serait tentant de se laisser emballer prématurément par des communicants audacieux : **Le calculateur quantique n'est pas encore une réalité industrielle**. Mais la recherche s'en approche asymptotiquement.

Le risque induit par les calculateurs quantiques touche de façon fondamentale la cryptographie asymétrique, car son présupposé (des calculs difficiles) qui était vrai avec des calculateurs classiques, se trouve invalidé par le calculateur quantique.

A l'inverse, **la cryptographie symétrique reste sûre, à condition d'utiliser des tailles de clef appropriées.**

En ce qui concerne les réponses au risque quantique, le consensus des autorités est défavorable à la Cryptographie Quantique, qui n'est pas jugée assez mûre pour lutter contre les calculateurs quantiques.

Au contraire, l'approche de la **Cryptographie Post Quantique fait l'unanimité,** et commence à apporter des solutions crédibles et résistantes. Le processus de normalisation de PQC du NIST est proche de sa conclusion. En attendant la disponibilité de ces nouvelles technologies, l'ANSSI propose des mesures intermédiaires, comme l'utilisation de systèmes hybrides.

L'apparition de fonctionnalités « quantiques » dans des produits grand public semble anecdotique. Leurs atouts ne semblent pas encore clairs, au risque d'utiliser « Quantique » comme un mantra destiné à attirer l'attention du marché, pour cacher le vide de la proposition.

Pour le spécialiste de cybersécurité, on peut en tirer quelques conséquences :

- **Il est indispensable de disposer de la culture générale qui permet d'exercer son esprit critique et analyser sérieusement les communications des acteurs.**
- **Il convient de réaliser une veille technologique régulière, dans un premier temps, basée sur la lecture de la presse grand public « informée, spécialisée » puis d'en confirmer les affirmations par la lecture académique.**
- **Un premier point critique est le support physique du qubit, avec 2 critères clef : le taux d'erreur et la densité de qubits.**
- **Un deuxième point critique est la technologie de correction d'erreur, et en particulier le taux de redondance**
- **Un troisième point potentiellement critique est la découverte de nouveaux algorithmes quantiques.**

Pour l'enseignant, formateur, consultant, on pourra rajouter :

- **La vulgarisation de ces domaines est très difficile, car les mathématiques tiennent une place prépondérante, l'expérimentation difficile à interpréter, le comportement des systèmes contre-intuitif.**
- **Il y a donc sûrement une place pour de l'enseignement vulgarisateur et peut-être un créneau de cours/formations sur les domaines étudiés.**
- **Les 2 domaines clefs à enseigner semblent être la QEC et la PQC**
- **On peut envisager de compléter les cours par des TPs, par exemple en utilisant les plateformes de simulation ou de calcul quantique proposés par les acteurs industriels.**

- **Il reste à trouver (ou créer ?) un blog ou une news-letter qui réalise une veille académique, technologique et industrielle sur le domaine. Peut-être une idée supplémentaire d'activité passionnante et utile, à défaut d'être directement rémunératrice.**

Cette conclusion ne serait pas complète sans l'évocation d'un des prolongements récents du calculateur quantique :

L'**internet quantique** se propose de faire pour internet la même révolution que le Calculateur Quantique produirait pour l'informatique classique. On y retrouve donc **tous** les thèmes abordés, en particulier *[Idée 14 Non-localité]*

Bien évidemment, l'internet quantique pose aussi de nombreux problèmes de cybersécurité, et propose, lui aussi, des solutions innovantes, qui se rapprochent de la QC. Le lecteur désireux d'approfondir ce domaine pourra dans un premier temps, se référer au numéro spécial de « Pour la science » (Collectif, 2021) dédié à ce sujet.

5 Bibliographie

Si le lecteur devait retenir une bibliographie courte mais complète, il pourrait choisir :

- **Le rapport Forteza** *(P.FORTEZA, 2020)*
- **Le rapport de l'académie des sciences Américaine** *(NAP, 2019)*
- **Le white paper N° 27 de l'ETSI** *('Implementation Security of Quantum Cryptography, Introduction, challenges, solutions.', 2018)*
- **Le rapport de l'ENISA sur la PQC** *(Post-Quantum Cryptography: Current state and quantum mitigation, 2021)*
- Les recommandations et avis de **l'ANSSI** *(ANSSI: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques., 2020)*
- La **lettre de veille cyber** *(Lionel Guillet, Permanent)* est toujours très pertinente, on peut gager que les problématiques de calcul quantique, de PQC et QC ne lui échapperont pas.
- Lorsque l'on sait quoi chercher, **Wikipédia** reste une ressource inestimable. Parfois, il vaut mieux lire la version anglaise, et toujours valider en croisant les informations avec des références académiques, que l'on trouvera sur Google Scholar
- *(Pour la Science - la science expliquée par ceux qui la font, 2022)* est une revue généraliste, dans laquelle mécanique et calculs quantiques, cryptographie, informatique théorique reviennent régulièrement.

- *(Opinions Libres, le blog d'Olivier Ezratty, 2022)* est toujours intéressant, bien que la cryptographie ne soit pas son seul sujet (ou alors, justement pour cela)

Cette bibliographie a été saisie, éditée et maintenue grâce à Zotero *(Zotero | Your personal research assistant, Permanent)* et son intégration avec MS-Word et LibreOffice. La grammaire et l'orthographe corrigés avec Grammalecte.

1. Alain Aspect (2016) 'Aspect: Le débat Einstein-Bohr est complètement clos', Pour la Science, Décembre 2016, pp. 22–25. Available at: https://www.pourlascience.fr/sd/histoire-sciences/le-debat-einstein-bohr-est-clos-9302.php.
2. Albert Einstein, Boris Podolsky et Nathan Rosen (1935) 'EPR: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?', *Physical Review Journals*, 47, pp. 777–780. Available at: https://journals.aps.org/pr/abstract/10.1103/PhysRev.47.777.
3. Alexander V. Sergienko (2006) *Quantum communications and cryptography*. CRC (Optical Science and Engineering). Available at: https://fr1lib.org/book/1023763/9c4a19.
4. Alice Sinatra (2008) *Sinatra: Introduction à la mécanique quantique*. (Cours de l'ENS). Available at: http://www.phys.ens.fr/~sinatra/cours.pdf.
5. 'ANSSI: Guide de sélection d'algorithmes cryptographiques' (2021). Available at: https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf.
6. *ANSSI: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.* (2020). Available at: https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques/ (Accessed: 24 November 2021).
7. A.Somoroff (2021) 'Extending superconducting qubit lifetimes: What's Next?', *Journal Club for Condensed Matter Physics* [Preprint]. Available at: https://www.condmatjclub.org/uploads/2021/09/JCCM_September_2021_01.pdf.
8. Aspect - Nature (1999) 'Aspect/Nature: Bell's inequality test: more ideal than ever', *Nature* [Preprint]. doi:10.1038/18296.
9. *Audition publique sur la stratégie quantique de la France* (2021) *videos.senat.fr*. Available at: http://videos.senat.fr/video.2549255_616f7a92e3f5b.audition-publique-sur-la-strategie-quantique-de-la-france (Accessed: 18 November 2021).
10. *Azure Quantum documentation, QDK & Q# API reference - Azure Quantum* (2022). Available at: https://docs.microsoft.com/en-us/azure/quantum/ (Accessed: 18 January 2022).
11. Bailly, S. (2012) *Le prix Nobel de physique 2012*, *Pour la Science, octobre 2012*. Pour la Science. Available at: https://www.pourlascience.fr/sd/physique/le-prix-nobel-de-physique-2012-a-serge-haroche-et-david-wineland-11451.php (Accessed: 17 January 2022).
12. Basdevant, J.-L., Dalibard, J. and Joffre, M. (2002) *Mécanique quantique, cours à l'école Polytechnique*. Editions Ecole Polytechnique.
13. Beky, A. (2022) *La France lance une plateforme de calcul quantique hybride*, *Silicon*. Available at: https://www.silicon.fr/france-plateforme-calcul-quantique-429430.html (Accessed: 26 January 2022).
14. Bellac, M.L. (2013) *Physique quantique - Fondements Tome 1: Fondements*. EDP Sciences (EDP Sciences/CNRS Editions). Available at: https://books.google.fr/books?id=LkfoHFPNCKEC.
15. Benjamin Lévi. (2004) 'Thèse: Simulation de systèmes quantiques sur un ordinateur quantique réaliste. Physique [physics]. Université Paris-Diderot - Paris VII, 2004. Français.' Available at: https://tel.archives-ouvertes.fr/tel-00007592.
16. Bonsack (1985) 'L'inégalité de Bell: démonstration intuitive et commentaires', *Dialectica*, 39(2), pp. 111–125. Available at: https://www.jstor.org/stable/42970535.

17. Boston Consulting Group (2021) Quantum Computing Set to Transform Multiple Industries, Create Up to $850 Billion in Annual Value by 2040, Latest Estimates Show, BCG Global. Available at: https://www.bcg.com/press/21july2021-quantum-computing-transform-multiple-industries-create-850-billion-annual-value (Accessed: 14 January 2022).

18. Braunstein, S.L. and Pirandola, S. (2012) 'Side-channel-free quantum key distribution', *Physical Review Letters*, 108(13), p. 130502. doi:10.1103/PhysRevLett.108.130502.

19. *Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium – CERT-FR* (2021). Available at: https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-010/ (Accessed: 7 December 2021).

20. Carlson, E.K. (2021) 'Far Fewer Qubits Required for "Quantum Memory" Quantum Computers', *Physics*, 14, p. s117. doi:10.1103/PhysRevLett.127.140503.

21. Castro, V. (2019) *« Suprématie quantique » : Google, IBM et un exploit informatique contesté*, *Frandroid*. Available at: https://www.frandroid.com/marques/google/635013_suprematie-quantique-google-ibm-et-un-exploit-informatique-conteste (Accessed: 10 January 2022).

22. CNRS (2021) *Protéger les bits quantiques de la décohérence grâce aux photons | INP*. Available at: https://www.inp.cnrs.fr/fr/cnrsinfo/proteger-les-bits-quantiques-de-la-decoherence-grace-aux-photons (Accessed: 14 January 2022).

23. Colaïtis, Battini, M.J. *et al.* (1995) 'P3I, a Multi-Paradigm Real-Time Video Engine', in Paker, Y. and Wilbur, S. (eds) *Image Processing for Broadcast and Video Production*. London: Springer (Workshops in Computing), pp. 52–71. doi:10.1007/978-1-4471-3035-2_5.

24. Collectif (2021) 'L'internet quantique', *Pour la Science n°528 - Octobre 2021*, October. Available at: https://www.pourlascience.fr/sd/informatique/https:https://www.pourlascience.fr/sd/informatique/pour-la-science-n0528-21894.php (Accessed: 17 January 2022).

25. 'Commission Sénatoriale: Note n°15 L'ordinateur quantique' (2019). Available at: http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2019_0069_note_ordinateurs_quantiques.pdf.

26. Computer Security Division, I.T.L. (2017) *NIST Post-Quantum Cryptography Standardization*, *CSRC | NIST*. Available at: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization (Accessed: 21 January 2022).

27. Computer Security Division, I.T.L. (2021) *Third PQC Standardization Conference | CSRC*, *CSRC | NIST*. Available at: https://csrc.nist.gov/Events/2021/third-pqc-standardization-conference (Accessed: 24 January 2022).

28. Craig S. Smith (2021) *Competing Visions Underpin China's Quantum Computer Race*, *IEEE Spectrum*. Available at: https://spectrum.ieee.org/alibaba-baidu-quantum-computer-race (Accessed: 18 January 2022).

29. *Cryptographie post-quantique | docs.digicert.com* (Permanent). Available at: https://docs.digicert.com/fr/certificate-tools/post-quantum-cryptography/ (Accessed: 14 December 2021).

30. *CSRC Presentation: Rainbow Round 3 Presentation | CSRC* (2021) *CSRC | NIST*. Available at: https://csrc.nist.gov/Presentations/2021/rainbow-round-3-presentation (Accessed: 24 January 2022).

31. *CWE - CWE-330: Use of Insufficiently Random Values (4.6)* (Permanent). Available at: https://cwe.mitre.org/data/definitions/330.html (Accessed: 15 November 2021).

32. *CWE - CWE-331: Insufficient Entropy (4.6)* (Permanent). Available at: https://cwe.mitre.org/data/definitions/331.html (Accessed: 15 November 2021).

33. *CWE - CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) (4.6)* (Permanent). Available at: https://cwe.mitre.org/data/definitions/335.html (Accessed: 15 November 2021).

34. *CWE - CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (4.6)* (Permanent). Available at: https://cwe.mitre.org/data/definitions/338.html (Accessed: 15 November 2021).

35. D. Deutsch. (1985) 'Quantum theory, the church-turing principle and the universal quantum computer.', *Proc. R. Soc. Lond. A 400, 97 (1985).* [Preprint]. Available at: https://www.cs.princeton.edu/courses/archive/fall04/cos576/papers/deutsch85.pdf.

36. Daniel J. Bernstein ·Johannes Buchmann (2008) *Post-Quantum Cryptography*. Available at: https://www.researchgate.net/profile/Nicolas-Sendrier-2/publication/226115302_Code-Based_Cryptography/links/540d62d50cf2df04e7549388/Code-Based-Cryptography.pdf.

37. DeCusatis, C. and Mcgettrick, E. (2021) 'Near term implementation of Shor's Algorithm using Qiskit', in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1564–1568. doi:10.1109/CCWC51732.2021.9376169.

38. Dustin Moody (2021) 'The Homestretch: the beginning of the end of the NIST PQC 3rd Round'. Available at: https://pqcrypto2021.kr/download/program/2.2_PQCrypto2021.pdf.

39. EPFL, Cours (2013) 'Chapitre 3: Algorithme de Deutsch et Jozsa', in. Available at: https://documents.epfl.ch/groups/i/ip/ipg/www/2011-2012/Traitement_Quantique_de_l_Information_II/algodj2012.pdf.

40. EPFL, Cours (2013) 'Chapitre 7: Factorisation et Algorithme de Shor', in. Available at: https://documents.epfl.ch/groups/i/ip/ipg/www/2013-2014/Traitement_Quantique_de_l_Information/algoshor2013-14.pdf.

41. ETSI White Paper No. 27 (2018) *Implementation Security of Quantum Cryptography, Introduction, challenges, solutions.* Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf.

42. Foasso, C. (2021) *Quand l'informatique était analogique*, *Pour la science N°552, Mars 2021*. Pour la Science. Available at: https://www.pourlascience.fr/sr/https:https://www.pourlascience.fr/sr/histoire-sciencesquand-l-informatique-etait-analogique-21546.php (Accessed: 10 January 2022).

43. France Culture, Jean Dalibard (2022) *Grand entretien avec Jean Dalibard*, *France Culture*. Available at: https://www.franceculture.fr/emissions/la-methode-scientifique/grand-entretien-avec-jean-dalibard (Accessed: 8 January 2022).

44. Frank Laloë (2018) 'Comprenons-nous vraiment la mécanique quantique ? Cours de Physique à l'ENS', January. Available at: https://www.phys.ens.fr/cours/notes-de-cours/fl-mq/mq.PDF.

45. *Fun MOOC: Introduction à la mécanique quantique* (Permanent) *FUN MOOC*. Available at: http://www.fun-mooc.fr/fr/cours/introduction-a-la-physique-quantique-partie-1/ (Accessed: 26 October 2021).

46. *Gendarmerie nationale: Veille Calculateur quantique et sécurité* (2020). Available at: https://www.gendarmerie.interieur.gouv.fr/onists/ressources-documentaires/veille-technologique/calculateur-quantique-et-securite (Accessed: 2 December 2021).

47. Google Cirq (2022) *Software | Google Quantum AI*. Available at: https://quantumai.google/software?hl=fr (Accessed: 18 January 2022).

48. Google datasheet (2021) 'Weber'. Available at: https://quantumai.google/hardware/datasheet/weber.pdf?hl=fr.

49. Google Quantum AI (2022) *Quantum AI*. Available at: https://quantumai.google/?hl=fr (Accessed: 18 January 2022).

50. Google Quantum AI Hardware (2022) *Quantum AI Hardware*, *Google Quantum AI*. Available at: https://quantumai.google/hardware?hl=fr (Accessed: 18 January 2022).

51. Grangier, P. (1986) *Etude expérimentale de propriétés non-classique de la lumière; interférences à un seul photon*. phdthesis. Université Paris Sud - Paris XI. Available at: https://pastel.archives-ouvertes.fr/tel-00009436 (Accessed: 19 December 2021).

52. Grollier, D.Q., Julie (2020) *Quand la spintronique imite le cerveau*, *Pour la science N° 515, Juillet 2020*. Pour la Science. Available at: https://www.pourlascience.fr/sd/technologie/https:https://www.pourlascience.fr/sd/technologie/quand-la-spintronique-imite-le-cerveau-19913.php (Accessed: 17 January 2022).

53. Grover, L.K. (1996) 'A fast quantum mechanical algorithm for database search', *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, July 1996. doi:https://doi.org/10.1145/237814.237866.

54. Haroche, S. (2016) *Il était deux fois la révolution quantique*, *DOSSIER POUR LA SCIENCE N° 93, octobre 2016*. Pour la Science. Available at: https://www.pourlascience.fr/theme/cryptographie/https:https://www.pourlascience.fr/theme/cryptographie/il-etait-deux-fois-la-revolution-quantique-9293.php (Accessed: 26 October 2021).

55. Heintzman, A.M., Douglas (2021) 'The Complex Path to Quantum Resistance', in. *Communications of the ACM, September 2021, Vol. 64 No. 9, Pages 46-53*. Available at: https://cacm.acm.org/magazines/2021/9/255037-the-complex-path-to-quantum-resistance/fulltext (Accessed: 25 January 2022).

56. Hemsoth, N. (2021) *Alibaba's Key to Cryptosecurity is Its Own Quantum Platform*, *The Next Platform*. Available at: https://www.nextplatform.com/2021/07/12/alibabas-key-to-cryptosecurity-is-its-own-quantum-platform/ (Accessed: 18 January 2022).

57. Huang, L. *et al.* (2021) 'Quantum random number cloud platform', *npj Quantum Information*, 7(1), pp. 1–7. doi:10.1038/s41534-021-00442-x.

58. *IBM Quantum breaks the 100-qubit processor barrier* (2021) *IBM Research Blog*. Available at: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle (Accessed: 10 January 2022).

59. IBM Quantum Computing (2022) *What is Quantum Computing?* Available at: https://www.ibm.com/topics/quantum-computing (Accessed: 18 January 2022).

60. IBM Quantum Computing, F.C. (2022) *IBM | Quantum Computing*, *IBM | Quantum Computing*. Available at: https://ibm.com/quantum-computing// (Accessed: 10 January 2022).

61. *IBM Quantum System One* (2018) *IBM Quantum System One*. Available at: https://research.ibm.com/ibm-q/qed/index.html (Accessed: 18 January 2022).

62. *IBM Research Blog | IBM Research* (2021) *IBM Research Blog*. Available at: https://research.ibm.com/blog?tag=quantum-computing (Accessed: 18 January 2022).

63. *IBM's roadmap for scaling quantum technology* (2021) *IBM Research Blog*. Available at: https://research.ibm.com/blog/ibm-quantum-roadmap (Accessed: 10 January 2022).

64. *ID Quantique* (2022) *ID Quantique*. Available at: https://www.idquantique.com/ (Accessed: 20 January 2022).

65. 'ID Quantique and SK Telecom announce the world's first 5G smartphone equipped with a Quantum Random Number Generator (QRNG) chipset' (2020) *ID Quantique*, 13 May. Available at: https://www.idquantique.com/id-quantique-and-sk-telecom-announce-the-worlds-first-5g-smartphone-equipped-with-a-quantum-random-number-generator-qrng-chipset/ (Accessed: 20 January 2022).

66. IDC (2021) *Quantum Computing Grows*, *IDC: The premier global market intelligence company*. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS47696021 (Accessed: 18 January 2022).

67. IEEE Quantum (2022) *Home - IEEE Quantum*. Available at: https://quantum.ieee.org/ (Accessed: 14 January 2022).

68. IEEE Spectrum (2021) *Quantum Randomness Now Boosts Everyday Security*, *IEEE Spectrum*. Available at: https://spectrum.ieee.org/quantum-randomness-boosts-everyday-security (Accessed: 20 January 2022).

69. Institut des Hautes Études Scientifiques (IHÉS) (2019) *Alain Aspect - Le photon onde ou particule ? L'étrangeté quantique mise en lumière*. Available at: https://www.youtube.com/watch?v=_kGqkxQo-Tw (Accessed: 9 November 2021).

70. Jeffrey Quilliam (2019) 'U-Sherbrooke: TP Inégalités de Bell'. Available at: https://tp.physique.usherbrooke.ca/notes_de_cours/Inegalites_de_Bell.pdf.

71. Jens Kröger (Permanent) *U-Laval, cours : Les inégalités de Bell*. Available at: http://feynman.phy.ulaval.ca/marleau/pp/03epr/epr_2/epr_2.html (Accessed: 4 November 2021).

72. Jintai Ding (2005) 'Rainbow, a New Multivariable Polynomial Signature Scheme', in Lecture Notes in Computer Science. Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings. doi:10.1007/11496137_12.

73. *Keeping information secure in the era of the quantum computer | Inria* (Permanent). Available at: https://www.inria.fr/en/keeping-information-secure-era-quantum-computer (Accessed: 25 January 2022).

74. 'La communication quantique et le protocole BB84 – Science étonnante' (2019), 14 February. Available at: https://scienceetonnante.com/2019/02/14/bb84/ (Accessed: 20 January 2022).

75. *La Corée du Nord a dérobé pour 400 millions de dollars de cryptos en 2021* (2022) *Les Echos*. Available at: https://www.lesechos.fr/finance-marches/marches-financiers/la-coree-du-nord-derobe-pour-400-millions-de-dollars-de-cryptos-en-2021-1379395 (Accessed: 19 January 2022).

76. *La France investit 1,8 milliard d'euros dans les technologies quantiques* (2021) *Futura*. Available at: https://www.futura-sciences.com/tech/actualites/ordinateur-quantique-france-investit-18-milliard-euros-technologies-quantiques-85283/ (Accessed: 26 January 2022).

77. *La plateforme française de calcul quantique est lancée* (2022) *Franceinfo*. Available at: https://www.francetvinfo.fr/replay-radio/le-billet-sciences-du-week-end/la-plateforme-francaise-de-calcul-quantique-est-lancee_4893217.html (Accessed: 8 January 2022).

78. 'La téléportation quantique' (2019) *|TheKetQuest>*, 9 February. Available at: https://theketquest.home.blog/la-teleportation-quantique/ (Accessed: 9 November 2021).

79. Laguillaumie, F., Langlois, A. and Stehlé, D. (2014) *Chiffrement avancé à partir du problème Learning With Errors*. Presses universitaires de Perpignan. Available at: https://hal.inria.fr/hal-00984055 (Accessed: 24 January 2022).

80. *L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés ?* (2020) *ANSSI*. Available at: https://www.ssi.gouv.fr/agence/publication/lavenir-des-communications-securisees-passe-t-il-par-la-distribution-quantique-de-cles/ (Accessed: 20 January 2022).

81. Le Bellac., M. (2006) 'Introduction à l'information quantique, cel-00092955, Cours donnée a l'Ecole Superieure de Sciences Informatiques'. Available at: cel.archives-ouvertes.fr/docs/00/09/29/55/PDF/cel-29.pdf.

82. Le Monde (2022) 'Cyberattaque : l'Ukraine accuse la Russie et dit avoir des « preuves »', *Le Monde.fr*, 16 January. Available at: https://www.lemonde.fr/pixels/article/2022/01/16/microsoft-a-detecte-une-attaque-visant-a-saboter-des-systemes-informatiques-de-l-etat-ukrainien_6109709_4408996.html (Accessed: 19 January 2022).

83. *Le Monde.fr* (2020) 'La suprématie quantique ou la nouvelle frontière des géants de l'informatique', 8 January. Available at: https://www.lemonde.fr/idees/article/2020/01/08/la-suprematie-quantique-ou-la-nouvelle-frontiere-des-geants-de-l-informatique_6025132_3232.html (Accessed: 10 January 2022).

84. Lenstra, A. *et al.* (2003) 'Factoring Estimates for a 1024-Bit RSA Modulus', in Laih, C.-S. (ed.) *Advances in Cryptology - ASIACRYPT 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 55–74. Available at: https://www.iacr.org/archive/asiacrypt2003/02_Session02/18_019/28940287.pdf.

85. *Les expériences d'Aspect (1980-1982)* (Permanent) *Techno-Science.net*. Available at: https://www.techno-science.net/glossaire-definition/Experience-d-Aspect-page-3.html (Accessed: 8 November 2021).

86. Lévy-Leblond, J.-M. (2017) *Qu'est donc le spin ?*, *Pour la science N° 473, février 2017*. Pour la Science. Available at: https://www.pourlascience.fr/sd/physique-particules/qu-est-donc-le-spin-9532.php (Accessed: 26 October 2021).

87. Lionel Guillet (Permanent) *Veille cyber*. Available at: https://veillecyberland.wordpress.com/ (Accessed: 25 January 2022).

88. *MagiQ QPN* (2022) *MagiQ Technologies*. Available at: https://www.magiqtech.com/solutions/network-security/ (Accessed: 20 January 2022).

89. *Microsoft Quantum Newsletter* (2022). Available at: https://azure.microsoft.com/en-us/solutions/quantum-computing/quantum-computing-newsletter-signup/ (Accessed: 18 January 2022).

90. *Microsoft Quantum overview* (2022). Available at: https://azure.microsoft.com/en-us/solutions/quantum-computing/ (Accessed: 10 January 2022).

91. *MITRE ATT&CK®* (Permanent). Available at: https://attack.mitre.org/ (Accessed: 15 November 2021).

92. *MOOC Mécanique quantique* (Permanent) *Coursera*. Available at: https://www.coursera.org/learn/mecanique-quantique (Accessed: 26 October 2021).

93. NAP (2019) Quantum Computing: Progress and Prospects (2019). National Academies of Sciences, Engineering, and Medicine. Consensus Study Report. Available at: https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects.

94. Ng Seth Lloyd, Y. Jack (2004) *L'Univers, un monstre informatique*, *POUR LA SCIENCE N° 325, novembre 2004*. Pour la Science. Available at: https://www.pourlascience.fr/sd/physique/l-univers-un-monstre-informatique-1582.php (Accessed: 14 January 2022).

95. *NSA Quantum Key Distribution (QKD) and Quantum Cryptography QC* (Permanent). Available at: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (Accessed: 25 January 2022).

96. *NSA Post-Quantum Cybersecurity Resources* (Permanent). Available at: https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/ (Accessed: 25 January 2022).

97. *On "Quantum Supremacy"* (2019) *IBM Research Blog*. Available at: https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/ (Accessed: 10 January 2022).

98. *Open Quantum Safe* (Permanent) *Open Quantum Safe*. Available at: https://openquantumsafe.org/ (Accessed: 25 January 2022).

99. *Opinions Libres, le blog d'Olivier Ezratty* (2022). Available at: https://www.oezratty.net/wordpress/ (Accessed: 25 January 2022).

100. Osman, A. *et al.* (2021) 'Simplified Josephson-junction fabrication process for reproducibly high-performance superconducting qubits', *Applied Physics Letters*, 118(6), p. 064002. doi:10.1063/5.0037093.

101. P.FORTEZA (2020) 'QUANTIQUE : LE VIRAGE TECHNOLOGIQUE QUE LA FRANCE NE RATERA PAS, Rapport de mission parlementaire.' Available at: https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf.

102. Physics World (2021) *All-in-one quantum key distribution system makes its debut*, *Physics World*. Available at: https://physicsworld.com/all-in-one-quantum-key-distribution-system-makes-its-debut/ (Accessed: 20 January 2022).

103. Pljonkin, A. and Singh, P. (2018) 'The Review of the Commercial Quantum Key Distribution System', in. *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018,* pp. 795–799. doi:10.1109/PDGC.2018.8745822.

104. *Post-Quantum Crypto Agility* (Permanent). Available at: https://cpl.thalesgroup.com/encryption/post-quantum-crypto-agility (Accessed: 25 January 2022).

105. *Post-Quantum Cryptography: Current state and quantum mitigation* (2021) *ENISA*. Available at: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation (Accessed: 21 January 2022).

106. *Pour la Science - la science expliquée par ceux qui la font* (2022). Available at: https://www.pourlascience.fr/ (Accessed: 25 January 2022).

107. *PQCRainbow* (2022). Available at: https://www.pqcrainbow.org/ (Accessed: 24 January 2022).

108. *QCE21 Home ● IEEE Quantum Week* (2021) *IEEE Quantum Week*. Available at: https://qce.quantum.ieee.org/ (Accessed: 14 January 2022).

109. *Qiskit* (2022). Available at: https://qiskit.org/ (Accessed: 18 January 2022).

110. *Quantum computing use cases--what you need to know | McKinsey* (2021). Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know (Accessed: 10 January 2022).

111. *Quantum Lab - DAMO Academy* (2022). Available at: https://damo.alibaba.com/labs/quantum (Accessed: 18 January 2022).

112. *Quantum Walks, Bell* (2018). Available at: http://www.promenades-quantiques.com/journal/lettres_2018/lettre_18_09/18-09-Inegalite-Bell-et-hasard.html (Accessed: 4 November 2021).

113. *Quantum Walks, EPR* (2018). Available at: http://www.promenades-quantiques.com/journal/lettres_2018/lettre_18_01/18-01-Argument-EPR-intrication.html (Accessed: 8 November 2021).

114. *Quantum Walks, Stern & Gerlach* (2013). Available at: http://www.promenades-quantiques.com/journal/lettres_2013/lettre_13_12/13-12-Stern-Gerlach.html (Accessed: 26 October 2021).

115. *Quantum Xchange | Thales* (2022). Available at: https://cpl.thalesgroup.com/partners/quantum-xchange (Accessed: 20 January 2022).

116. *Qubit : définition et explications* (2021) *Techno-Science.net*. Available at: https://www.techno-science.net/definition/8041.html (Accessed: 10 January 2022).

117. *Qu'est-ce que l'informatique quantique ?* (Permanent). Available at: https://www.ibm.com/fr-fr/topics/quantum-computing (Accessed: 10 January 2022).

118. *RETEX ECW21 : Mise en œuvre de la cryptographie post-quantique* (2021) *ACCEIS*. Available at: https://www.acceis.fr/retex-ecw21-mise-en-oeuvre-de-la-cryptographie-post-quantique/ (Accessed: 6 December 2021).

119. Roffe, J. (2019) 'Quantum Error Correction: An Introductory Guide', *Contemporary Physics*, 60(3), pp. 226–245. doi:10.1080/00107514.2019.1667078.

120. Sabine Hossenfelder (2021) *Quantum Computing: Top Players 2021*. Available at: https://www.youtube.com/watch?v=OGsu5MIzruw (Accessed: 14 January 2022).

121. Sacco, L. (2021) *Internet quantique : la Chine réalise la première transmission entre un satellite et un récepteur mobile*, *Futura*. Available at: https://www.futura-

sciences.com/sciences/actualites/physique-internet-quantique-chine-realise-premiere-transmission-satellite-recepteur-mobile-38796/ (Accessed: 9 November 2021).

122. ScienceEtonnante (2020) *Alain Aspect : Intrication quantique et inégalités de Bell [Interview complète]*. Available at: https://www.youtube.com/watch?v=OeZ_63iKPho (Accessed: 8 November 2021).

123. Serge Haroche (Permanent) 'Cours au collège de France'. Available at: https://www.college-de-france.fr/site/serge-haroche/_course.htm.

124. Serge Haroche, prix Nobel de physique 2012 - La Chancellerie des Universités de Paris (2012) La Chancellerie des Universités de Paris. Available at: https://www.sorbonne.fr/serge-haroche-prix-nobel-de-physique-2012/ (Accessed: 14 January 2022).

125. Service d'informatique quantique | Amazon Braket | Amazon Web Services (2022) Amazon Web Services, Inc. Available at: https://aws.amazon.com/fr/braket/ (Accessed: 18 January 2022).

126. Sharma, P. *et al.* (2021) 'Quantum Key Distribution Secured Optical Networks: A Survey', *IEEE Open Journal of the Communications Society*, 2, pp. 2049–2083. doi:10.1109/OJCOMS.2021.3106659.

127. Shor, P.W. (1997) 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *SIAM Journal on Computing*, 26(5), pp. 1484–1509. doi:10.1137/S0097539795293172.

128. sifted (2022) *Dozens of companies budget $1m+ for quantum computing as tech race intensifies*, *Sifted*. Available at: https://sifted.eu/articles/companies-spending-quantum-computing/ (Accessed: 18 January 2022).

129. Sophian Teber (no date) 'Cours de Sorbonne Université, Master de Sciences et Technologie, Mécanique Quantique (4P001)'. Available at: https://www.lpthe.jussieu.fr/~teber/Teaching/poly.pdf.

130. *Spin : définition et explications* (Permanent) *Techno-Science.net*. Available at: https://www.techno-science.net/definition/8044.html (Accessed: 8 November 2021).

131. Struyve, W. (2020) *Une réalité classique derrière l'étrangeté quantique ?*, *Pour la Science N° 509, Février 2020*. Pour la Science. Available at: https://www.pourlascience.fr/https:https://www.pourlascience.fr/une-realite-classique-derriere-l-etrangete-quantique-18878.php (Accessed: 8 November 2021).

132. *Superposition – Tout est quantique* (2021). Available at: https://toutestquantique.fr/superposition/ (Accessed: 9 November 2021).

133. Sylvain Larroque (2020) *L'expérience des doubles fentes d'Young avec un canon à électrons*, *Université de Bordeaux, Unité de formation de physique*. Available at: http://physique.u-bordeaux.fr/Espaces-etudiants/Doctorat/L-experience-des-doubles-fentes-d-Young-avec-un-canon-a-electrons (Accessed: 29 October 2021).

134. Sylvain Nadeau (Permanent) *U-Laval, cours: LES EXPÉRIENCES D'ASPECT*. Available at: http://feynman.phy.ulaval.ca/marleau/pp/03epr/epr_3/epr_3.html (Accessed: 8 November 2021).

135. Technology, N.I. of S. and (2002) *Security Requirements for Cryptographic Modules*. Federal Information Processing Standard (FIPS) 140-2. U.S. Department of Commerce. doi:10.6028/NIST.FIPS.140-2.

136. Télécom ParisTalks 'Ordinateur quantique et cryptographie post-quantique : quand l'ingénierie prendra t'elle la place de la recherche ?' (2021). Available at: https://executive-education.telecom-paris.fr/fr/agenda/telecom-paristalks-ordinateur-quantique-et-cryptographie-post-quantique-quand-lingenierie (Accessed: 25 January 2022).

137. *The current state of quantum computing: Between hype and revolution* (2021). Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/the-current-state-of-quantum-computing-between-hype-and-revolution (Accessed: 18 January 2022).

138. *The Home of Scalable IoT Security* (2022) *Crypto Quantique*. Available at: https://www.cryptoquantique.com/ (Accessed: 20 January 2022).

139. *The Quantum Insider* (2022) *The Quantum Insider*. Available at: https://thequantuminsider.com/ (Accessed: 18 January 2022).

140. *TQI - Making Quantum Computing accessible through media and data* (Permanent) *The Quantum Insider*. Available at: https://thequantuminsider.com/ (Accessed: 25 January 2022).

141. Trust My Science (2021) *Estimation de la quantité d'information contenue dans l'Univers observable, Trust My Science*. Available at: https://trustmyscience.com/chercheur-propose-estimation-information-contenue-dans-matiere-visible-univers/ (Accessed: 14 January 2022).

142. Wikipédia (2021) 'Informatique réversible - Reversible computing Informatique réversible -'. Available at: https://fr.abcdef.wiki/wiki/Reversible_computing.

143. *Wikipedia - Born rule* (Permanent). Available at: https://fr.abcdef.wiki/wiki/Born_rule (Accessed: 10 January 2022).

144. 'Wikipédia: Algorithme de Grover' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Algorithme_de_Grover&oldid=183798877 (Accessed: 18 January 2022).

145. 'Wikipedia: Algorithme de Shor' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Algorithme_de_Shor&oldid=180787047 (Accessed: 11 January 2022).

146. 'Wikipedia: Calcul quantique adiabatique' (2018) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Calcul_quantique_adiabatique&oldid=154716922 (Accessed: 17 January 2022).

147. 'Wikipédia: Calculateur quantique' (2022) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Calculateur_quantique&oldid=189747102 (Accessed: 10 January 2022).

148. 'Wikipedia: Catastrophe ultraviolette' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Catastrophe_ultraviolette&oldid=186343066 (Accessed: 26 October 2021).

149. 'Wikipédia: Chiffrement RSA' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Chiffrement_RSA&oldid=188508333 (Accessed: 11 January 2022).

150. 'Wikipédia: Cryptographie post-quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Cryptographie_post-quantique&oldid=186616698 (Accessed: 21 January 2022).

151. 'Wikipédia: Cryptographie quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Cryptographie_quantique&oldid=185721676 (Accessed: 20 January 2022).

152. 'Wikipédia: Cryptographie sur les courbes elliptiques' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Cryptographie_sur_les_courbes_elliptiques&oldid=184519230 (Accessed: 19 January 2022).

153. 'Wikipédia: Cryptosystème de McEliece' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Cryptosyst%C3%A8me_de_McEliece&oldid=188135623 (Accessed: 21 January 2022).

154. 'Wikipédia: Décohérence quantique' (2020) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=D%C3%A9coh%C3%A9rence_quantique&oldid=176290796 (Accessed: 29 October 2021).

155. 'Wikipedia: Dualité onde-corpuscule' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Dualit%C3%A9_onde-corpuscule&oldid=185598586 (Accessed: 29 October 2021).

156. 'Wikipedia: Effet photoélectrique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Effet_photo%C3%A9lectrique&oldid=184076091 (Accessed: 26 October 2021).

157. 'Wikipédia: Équation de Schrödinger' (2022) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=%C3%89quation_de_Schr%C3%B6dinger&oldid=189708620 (Accessed: 10 January 2022).

158. 'Wikipedia: Expérience d'Aspect' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Exp%C3%A9rience_d%27Aspect&oldid=183938278 (Accessed: 8 November 2021).

159. 'Wikipedia: Expériences sur les inégalités de Bell' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Exp%C3%A9riences_sur_les_in%C3%A9galit%C3%A9s_de_Bell&oldid=185327471 (Accessed: 8 November 2021).

160. 'Wikipedia: Fentes de Young' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Fentes_de_Young&oldid=183913210 (Accessed: 29 October 2021).

161. 'Wikipedia: Histoire de la mécanique quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Histoire_de_la_m%C3%A9canique_quantique&oldid=184313060 (Accessed: 26 October 2021).

162. 'Wikipédia: Impossibilité du clonage quantique' (2014) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Impossibilit%C3%A9_du_clonage_quantique&oldid=103022000 (Accessed: 14 January 2022).

163. 'Wikipedia: Inégalités de Bell' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=In%C3%A9galit%C3%A9s_de_Bell&oldid=182306142 (Accessed: 5 November 2021).

164. 'Wikipédia: Information quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Information_quantique&oldid=183590354 (Accessed: 29 November 2021).

165. 'Wikipédia: Informatique quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Informatique_quantique&oldid=183688499 (Accessed: 10 January 2022).

166. 'Wikipédia: Integer factorization' (2021) *Wikipedia*. Available at: https://en.wikipedia.org/w/index.php?title=Integer_factorization&oldid=1057170623 (Accessed: 11 January 2022).

167. 'Wikipedia: Introduction à la mécanique quantique' (2020) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Introduction_%C3%A0_la_m%C3%A9canique_quantique&oldid=176930262 (Accessed: 26 October 2021).

168. 'Wikipedia: Mécanique quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=M%C3%A9canique_quantique&oldid=186002978 (Accessed: 26 October 2021).

169. 'Wikipedia: Nombre quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Nombre_quantique&oldid=186539892 (Accessed: 29 October 2021).

170. 'Wikipédia: Notation bra-ket' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Notation_bra-ket&oldid=181741844 (Accessed: 29 November 2021).

171. 'Wikipédia: Observable' (2022) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Observable&oldid=189506141 (Accessed: 10 January 2022).

172. 'Wikipedia: Paradoxe EPR' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Paradoxe_EPR&oldid=186804813 (Accessed: 5 November 2021).

173. 'Wikipédia: Porte de Toffoli' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Porte_de_Toffoli&oldid=185386108 (Accessed: 10 January 2022).

174. 'Wikipédia: Post-quantum cryptography' (2021) *Wikipedia*. Available at: https://en.wikipedia.org/w/index.php?title=Post-quantum_cryptography&oldid=1062342218 (Accessed: 10 January 2022).

175. 'Wikipédia: Principe de superposition quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Principe_de_superposition_quantique&oldid=182311016 (Accessed: 5 November 2021).

176. 'Wikipedia: Principe d'exclusion de Pauli' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Principe_d%27exclusion_de_Pauli&oldid=186466271 (Accessed: 26 October 2021).

177. 'Wikipedia: Principe d'incertitude' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Principe_d%27incertitude&oldid=187736139 (Accessed: 9 November 2021).

178. 'Wikipedia: Problème de la mesure quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Probl%C3%A8me_de_la_mesure_quantique&oldid=182305852 (Accessed: 29 October 2021).

179. 'Wikipédia: Protocole BB84' (2020) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Protocole_BB84&oldid=176519479 (Accessed: 20 January 2022).

180. 'Wikipédia: Quantum decoherence' (2022) *Wikipedia*. Available at: https://en.wikipedia.org/w/index.php?title=Quantum_decoherence&oldid=1063201216 (Accessed: 3 January 2022).

181. 'Wikipedia: Spin' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Spin&oldid=187054722 (Accessed: 26 October 2021).

182. 'Wikipédia: Suprématie quantique' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Supr%C3%A9matie_quantique&oldid=188364658 (Accessed: 10 January 2022).

183. 'Wikipedia: Théorie de De Broglie-Bohm' (2021) *Wikipédia*. Available at: https://fr.wikipedia.org/w/index.php?title=Th%C3%A9orie_de_De_Broglie-Bohm&oldid=181303156 (Accessed: 8 November 2021).

184. Wu, A. *et al.* (2021) 'Mapping Surface Code to Superconducting Quantum Processors', *arXiv:2111.13729 [quant-ph]* [Preprint]. Available at: http://arxiv.org/abs/2111.13729 (Accessed: 19 January 2022).

185. Yahoo! news (2021) *Behind in quantum computer race, Germany gets boost from IBM*. Available at: https://news.yahoo.com/behind-quantum-compute-race-germany-132453704.html (Accessed: 18 January 2022).

186. Yanofsky, N.S. and Mannucci, M.A. (2008) *Quantum Computing for Computer Scientists*. 1er édition. Cambridge: Cambridge University Press.

187. *Zotero | Your personal research assistant* (Permanent). Available at: https://www.zotero.org/ (Accessed: 26 October 2021).