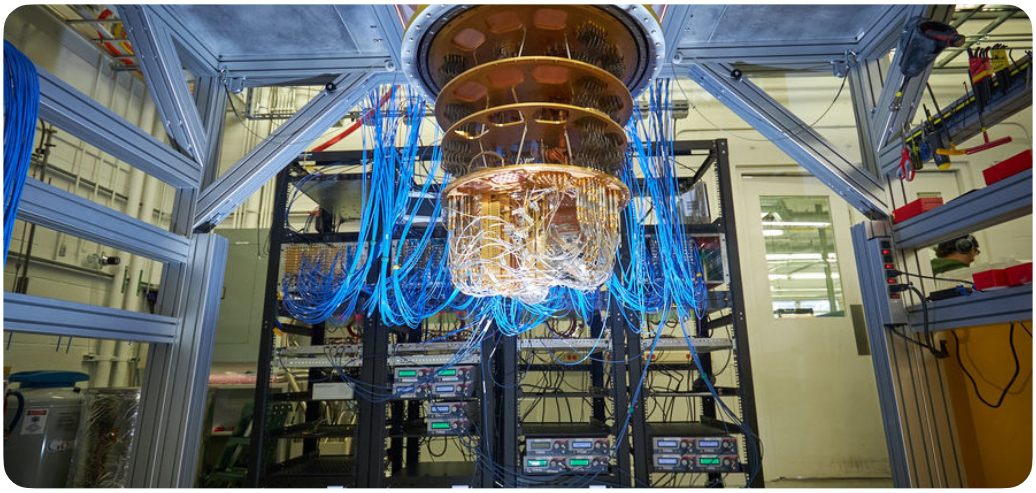
1. Qu'est-ce qu'un Ordinateur Quantique ?

Définition d'un ordinateur quantique : Un ordinateur quantique est équivalent à un ordinateur classique mais qui effectue ses calculs en utilisant directement les lois de la physique quantique. Alors qu'un ordinateur classique manipule des 1 (Vrai) ou des 0 (Faux) (**bits**), un ordinateur quantique lui utilise des 1 des 0 ou les deux à la fois(superposition simultanée des deux états vrai et faux) on appelle ça des **qubits**. De ce fait un ordinateur quantique peut faire des calculs beaucoup plus rapidement qu'un ordinateur classique.



Le plus puissant calculateur quantique de Google, Sycamore.

Définition de la physique quantique : La physique quantique a été créé à l'aube du 20ème siècle car les physiciens de l'époque réalisent que la physique classique, qui décrit parfaitement notre environnement quotidien **macroscopique** (qui se voit à l'œil nu), devient inefficace à l'échelle **microscopique** des atomes et des particules. En effet, les atomes et les particules élémentaires de la matière, n'évoluent pas comme un système macroscopique. Globalement pour imagez un atome en physique classique ne peut pas faire deux choses(1 seul état) en même temps alors qu'un atome en physique quantique lui peut le faire (être dans plusieurs états). La physique quantique contient trois valeurs : vrai, faux, et indéterminé au sens du principe d'indétermination de Heisenberg.)

Histoire de la suprématie quantique : Dès **1981**, Richard Feynman(un physicien américain qui à réaliser des travaux sur le quantique)était convaincu que les ordinateurs quantiques offriraient une puissance de calcul considérablement supérieure à celle des ordinateurs numériques. L'idée d'une « Suprématie Quantique » a été évoquée par John Preskill (un physicien théoricien américain qui à réaliser des travaux sur le calcul quantique) en **2011** pour lui « l'ère où la suprématie quantique débutera lorsqu'il sera démontrée qu'un ordinateur quantique sera plus performant que l'ordinateur (supercalculateurs) le plus puissant et avancé au monde. Par exemple les ingénieurs de Google, aidés par la Nasa et le laboratoire national d'Oak Ridge, affirment avoir réussi en **2020** à créer un processeur capable de réaliser un calcul en 200 secondes quand le plus avancé des ordinateurs actuels aurait besoin de 10.000 ans. (Données publiées en avril 2020).

Fugaku 415-PFLOPS le supercalculateur le plus puissant au monde.

Les entreprises qui développent des technologies quantique : Les principales entreprises qui sont à la pointe du quantique et développent leurs propres technologies sont Google, IBM, Intel, Microsoft et la NASA aux États Unis. En France, c'est Thales, Atos et Air liquide qui développent principalement des technologies dans le domaine.

Ce que va changer le quantique dans l'informatique et dans la vie quotidienne ? : L'ordinateur quantique pourra résoudre des problèmes complexes dans de nombreux domaines. C'est cette possibilité d'emprunter un nombre gigantesque de chemins qui rend les ordinateurs quantiques bien plus rapides que les ordinateurs classiques. Les ordinateurs quantiques seront utilisés pour différents types de problèmes, dans lesquels l'élimination d'un large éventail de possibilités permettra de gagner énormément de temps grâce à sa vitesse et ces performances. Un ordinateur quantique pourrait par exemple permettre d'inventer des molécules, de simuler de nouveaux matériaux, de créer de nouveaux médicaments, simuler le fonctionnement de l'univers, mieux prédire la météo, trouver de nouvelles planètes habitables.

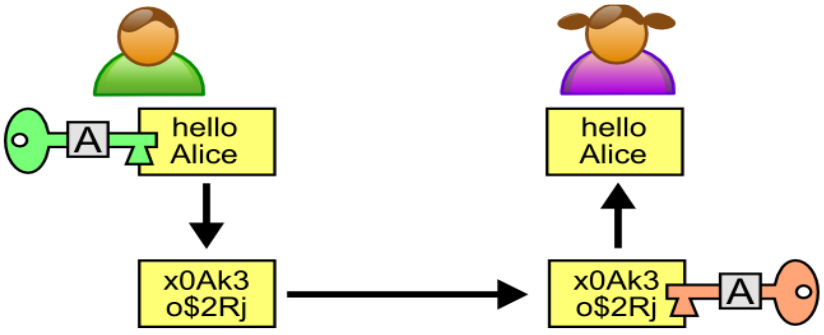
2. Cryptographie Quantique

Définition de la cryptographie : La cryptographie permet de chiffrez/protéger des messages en remplacent les caractères d'un message en plusieurs caractères qui se compose de lettres, chiffres, et caractères spéciaux.
Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie chiffre un message.

Définition de la cryptographie quantique : La cryptographie quantique consiste à utiliser les propriétés de la physique quantique permettant de garantir un secret absolu en chiffrant des messages par exemple et en garantissant des communications totalement cryptées et sécurisées entre les utilisateurs.

Applications de la cryptographie quantique : La cryptographie quantique a été mis en pratique pour la première fois en 2004 pour une importante transaction financière requérant une sécurité absolue et en 2007 lorsque l'entreprise suisse ID-Quantique a transmis les résultats des élections nationales à Genève. La cryptographie quantique intéresse également les militaires. La Darpa (agence américaine sur la recherche militaire avancée) utilise ainsi depuis 2004 un réseau de distribution quantique des clefs entre deux interlocuteurs (qui chiffre un message, et/ou des données confidentielles entre deux interlocuteurs).

Distribution quantique de clé : L'échange quantique de clé (QKD) est une distribution d'une clé unique entre deux utilisateurs qui communiquent sur un canal. Cette clé commune permet ensuite aux participants de chiffrer leurs communications au moyen d'un algorithme de chiffrement. Pour imager mon exemple Bob veut écrire un message à Alice. En envoyant son message, le contenu de son message se crypte et une clé **A** se crée pour sécuriser la communication entre Bob et Alice. Ensuite le message se décrypte pour qu'Alice puissent lire le message de Bob.

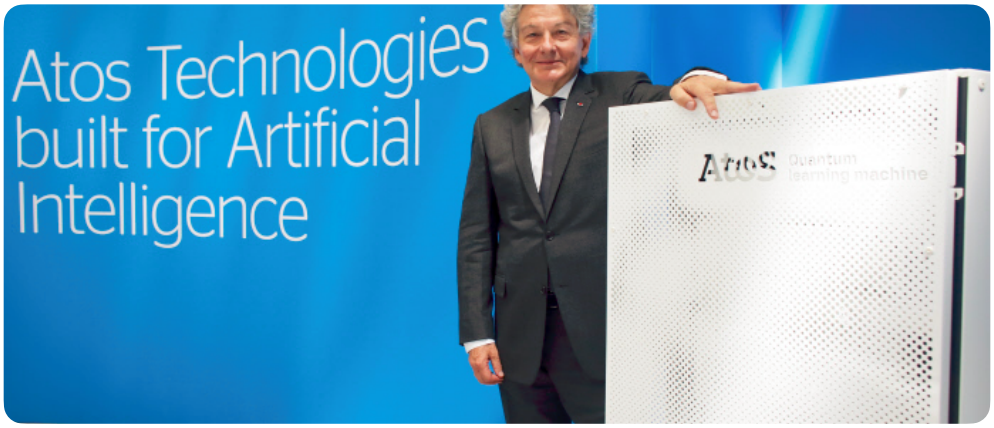


3. Simulateur Quantique

Définition d'un simulateur quantique : Un simulateur quantique est une classe restreinte d'ordinateur quantique que l'on peux exécuter sur des ordinateurs classiques et ont pour principale but de simuler un environnement de développement pour le quantique et pourront être ainsi utiliser pour prédire le comportement des qubits en réponse à différentes opérations.

Simulateur quantique existants :

- ATOS propose depuis 2017 un simulateur quantique reposant sur des serveurs classiques (à base de GPU NVIDIA) : le QLM (Quantum Learning Machine). QLM et est un simulateur d'ordinateur quantique à portes universelles. Disponible en 5 configurations de puissance (de 30 à 40 Qubits) pour couvrir les différents besoins des organisations, Atos QLM permet aux chercheurs, étudiants et ingénieurs de développer et tester dès à présent les applications et algorithmes quantiques de l'ordinateur de demain.



Simulateur quantique d'Atos

- **Microsoft** a lancé en décembre 2017 un simulateur quantique Quantum (**QDK**) et un kit de développement avec un langage de programmation spécifique au domaine appelé **Q#**.

- **IBM** propose également un kit de développement open source(que tout le monde peut voir et/ou modifier le code) appelé **Qiskit**, et permet aux utilisateur d'expérimenter la production d'algorithmes quantiques à l'aide de son simulateur 32 qubit.