QUÉBEC QUANTIQUE

Catalyseur de l'écosystème quantique du Québec

quebec-quantique.ca

Lexique

Technologies quantiques

Informatique quantique

L'informatique quantique englobe les technologies de traitement de données qui utilisent les propriétés quantiques de la matière, telles que la superposition et l'intrication afin de procéder à des opérations sur des données. Cette façon de fonctionner permet d'effectuer, dans certains cas, des calculs plus rapides, plus efficaces et qui consomment moins d'énergie. Cette technologie ne remplacera pas les processeurs électroniques communément utilisés aujourd'hui, mais desservira certaines applications où l'avantage de performance offert sera pertinent.

Communication quantique

La communication quantique représente la transmission de toutes données qui utilisent un réseau ou un chiffrement quantique. Ce type de communication rend les données inviolables, et dans certains cas permet de transmettre des données déjà formatées pour le traitement pas des appareils quantiques.

Capteur quantique

Un capteur quantique est un équipement qui utilise un phénomène quantique afin d'interagir avec le monde physique et en prélever une mesure. Ces capteurs offrent un avantage face aux capteurs classiques, soit en sensibilité, en réduction du bruit ambiant, ou tout simplement en fournissant une richesse d'information qui est autrement impossible à obtenir.

Technologies habilitantes

Les technologies habilitantes englobent de nouveaux procédés et de nouvelles techniques qui permettent le développement et l'utilisation des technologie quantiques. Par exemple, nous comptons les technologies de l'information et des communications (TIC), les nanotechnologies et l'optique-photonique. Il est aussi possible d'inclure les technologies dites quantiques 1.0 dans ce sous-secteur.

Fiche créée en collaboration avec NUMANA Catalyseur d'écosystèmes technologiques

Partenaire public Québec

Distribution quantique de clés (*Quantum key distribution (QKD)*)

La distribution de clés quantiques est un concept de cybersécurité qui fonctionne en échangeant des clés cryptographiques encodées dans des propriétés quantiques. Contrairement au chiffrement classique, il est impossible d'intercepter la clé de déchiffrement d'un message sans enfreindre les lois de la physique, ce qui rend cette technologie fondamentalement sécuritaire. Une application complète de la distribution de clés quantiques nécessite des logiciels et des équipements qui travaillent de pair.

Cryptographie sécuritaire quantique (*Quantum safe cryptography (QSC)*)

La cryptographie sécuritaire quantique est une approche complémentaire à la distribution de clés quantiques. L'objectif reste de sécuriser les données contre des attaques quantiques, mais sans nécessiter des logiciels ou des équipements quantiques. Cette approche fonctionne en utilisant des algorithmes de chiffrement qui résistent à la fois aux capacités d'un processeur électronique d'un processeur quantique. L'avantage principal de cette technologie est qu'elle est implémentée entièrement au niveau des logiciels, ce qui rend la migration plus facile et moins couteuse. Dans un avenir très proche, il faudra sécuriser tous les réseaux, classiques ou quantiques, avec cette technologie.

Cryptographie post-quantique

Ce nom est aussi utilisé pour la cryptographie sécuritaire quantique. Le principe et le fonctionnement sont identiques, et il en résulte un réseau classique protégé contre les attaques quantiques.

Réseaux optimisés quantiques

Ce type de réseau promet d'être mature dans un avenir rapproché et permettra d'optimiser des processus pour l'informatique, le traitement de données et la communication quantiques.

Algorithmes quantiques hybrides

Ce type d'algorithmes s'exécute partiellement sur un processeur électronique et partiellement sur un processeur quantique. Comme le processeur quantique ne se spécialise que sur certains algorithmes, une solution complète de calcul nécessitera l'accès aux deux types de processeurs pour optimiser les ressources.

Calculs quantiques hybrides

Les calculs quantiques hybrides représentent les opérations effectuées par les algorithmes quantiques hybrides. Ils offrent les mêmes avantages et sont, à toutes fins pratiques, tributaires de la même technologie.

Algorithmes quantiques distribués

Ces algorithmes fonctionnent de façon similaire aux algorithmes quantiques hybrides à la différence que les données et la charge de calcul à accomplir peuvent être distribués sur plusieurs machines, qu'elles soient quantiques ou classiques. Cette solution permettra l'accès à des machines plus puissantes pour plus d'utilisateurs, vu qu'il serait trop couteux d'installer un ordinateur quantique chez chaque utilisateur potentiel. Les algorithmes quantiques distribués requerront un réseau capable de communication quantiques et classique, que ce soit à courte ou longue distance.

Calculs quantiques distribués

Les calculs quantiques distribués représentent les opérations effectuées par les algorithmes quantiques distribués. Ils offrent les mêmes avantages et sont, à toutes fins pratique, tributaire de la même technologie.