

Les promesses des technologies quantiques

Autor(en): **Saraga, Daniel**

Objektyp: **Article**

Zeitschrift: **Horizons : le magazine suisse de la recherche scientifique**

Band (Jahr): **28 (2016)**

Heft 110

PDF erstellt am: **06.08.2024**

Persistenter Link: <https://doi.org/10.5169/seals-772063>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Les promesses des technologies quantiques

Basées sur les propriétés étonnantes du monde microscopique, de nouvelles approches développent des systèmes de cryptage inviolables et rêvent d'ordinateurs surpuissants.

Texte: Daniel Saraga
Infographie: onlab, Thibaud Tissot

Gravitation
Basés sur la nature ondulatoire de la matière, des interféromètres atomiques peuvent détecter d'infimes changements dans le champ gravitationnel. Applications: gyroscopes pour navigation inertielle ou relevés géologiques.

Horloges
Des montres recourant à des qubits intriqués sont déjà plus précises que les horloges atomiques classiques utilisées dans les satellites GPS ou définissant la durée officielle d'une seconde.

Microscopie
Un dispositif d'imagerie utilisant des photons intriqués pourrait améliorer la microscopie en faible luminosité.

Capteur magnétique
Un défaut de cristal de diamant agit comme un atome artificiel sensible à des champs magnétiques extrêmement faibles, utile pour l'imagerie médicale ou la prospection pétrolière. Ce capteur pourrait remplacer les SQUID, une technologie quantique ne fonctionnant qu'à -170 °C.

Chiffrement
Le cryptage quantique a été démontré avec des fibres optiques sur des distances de plus de 100 kilomètres. La Chine a lancé un satellite en août 2016 afin de tester le chiffrement quantique via satellite.

Communication
Sécuriser les messages

Détection quantique
Dépasser les limites

Détection quantique
La nature ondulatoire de la matière est très sensible à l'environnement. Mesurer la rapidité avec laquelle elle disparaît (la décohérence) permet de quantifier des signaux extrêmement faibles.

Communication quantique
Des photons (des particules de lumière) intriqués peuvent être utilisés pour le cryptage. Un émetteur et un récepteur créent et partagent instantanément une succession aléatoire de bits (011011101011...) utilisables comme clé pour chiffrer un message. Ce dernier est transmis de manière conventionnelle, mais seul le récepteur, qui détient l'unique copie de la clé, peut le décoder.

Ordinateurs quantiques
L'information stockée sous forme de bits quantiques (qubit) est très fragile. L'intrication et le parallélisme quantiques permettent en principe de résoudre plus rapidement certains problèmes que les ordinateurs classiques.

Internet quantique
La transmission longue distance de qubits pourrait sous-tendre un réseau Internet sécurisé. Compenser les pertes de signal exigerait d'inventer des répéteurs quantiques, et de meilleurs détecteurs et sources de photons uniques seraient nécessaires pour augmenter la bande passante.

Une Suisse quantique



Doté d'un budget de 115 millions de francs pour la période 2011-2018, le PRN «QIT – Science et technologie quantiques» rassemble cinq universités et IBM Zurich.
L'Université de Genève et sa start-up ID Quantique sont des leaders mondiaux en cryptographie quantique.
L'Université de Bâle est pionnière en matière d'ordinateurs quantiques à base de semi-conducteurs et de détection à l'échelle atomique.
Des chercheurs de l'ETH Zurich développent des ordinateurs quantiques, corrigent des failles en cryptographie et sont des experts de la technologie de D-Wave.

Une machine universelle
Un véritable ordinateur quantique pourrait en plus résoudre des problèmes algébriques (utiles pour décoder les systèmes de chiffrement actuels) et rechercher les bases de données. Il exigerait des millions de qubits adressables individuellement.

Simulateurs quantiques
Un ordinateur quantique basique pourra simuler parfaitement d'autres systèmes moléculaires en chimie et science des matériaux, une tâche impossible actuellement. Des quantum annealers pourraient résoudre des problèmes d'optimisation (comme trouver le meilleur itinéraire ou horaire).

Premiers pas
Les meilleurs appareils de laboratoire peuvent contrôler une douzaine de qubits seulement. L'entreprise D-Wave loue des machines avec 1152 qubits, mais sans avoir pu démontrer son utilité.

quantique
les messages

Des étranges propriétés

Ondes et particules
De très petits objets tels qu'électrons, atomes ou photons affichent un comportement quantique dont on peut tirer parti, à condition qu'ils restent extrêmement bien isolés de leur environnement.

Information quantique
De l'information digitale peut être stockée dans des bits quantiques (qubits), définis par exemple par le sens de rotation d'un électron ou les niveaux d'énergie d'un atome.

Superposition
Un qubit peut représenter à la fois un 0 et un 1 en même temps, avec des rapports arbitraires.

Parallélisme
Plusieurs qubits peuvent être manipulés en même temps.

Intrication
Des qubits intriqués partagent un lien intrinsèque: mesurer l'un affecte automatiquement l'autre, peu importe leur éloignement.

Ordinateurs quantiques
Calculer avec des qubits

IBM Research
Quantum Inspire
D-Wave Systems
Google