Documents sauvegardés

Jeudi 5 février 2026 à 0 h 41

5 documents

Sommaire

Documents sauvegardés • 5 documents

Documents sauvegardés

Forbes (France) (site web) - Forbes.fr

Nom de la source
Forbes (France) (site web) - Forbes.fr

Type de source
Presse • Presse Web

Périodicité
En continu

Couverture géographique
Nationale

Provenance
Paris, Ile-de-France, France

Thursday, January 15, 2026

Forbes (France) (site web) - Forbes.fr • 1336 mots

LexisNexis

L'ordinateur quantique : Le nouveau défi de gouvernance que les conseils d'administration ne peuvent plus ignorer

Contribution

Catégorie : TechnologieUne contribution de Valérie Pilcer, Administratrice indépendante, experte en gouvernance et en IA générative pour dirigeants Pour un administrateur, il n'est plus nécessaire d'avoir un doctorat en physique pour comprendre les impacts du quantique, mais il est crucial d'en saisir le potentiel et la portée. L'informatique classique repose sur le "bit", l'unité d'information la plus simple, qui peut être soit 0, soit 1. Imaginez un labyrinthe : un ordinateur classique testerait chaque chemin l'un après l'autre jusqu'à trouver la sortie. Le qubit exploite la superposition des états : comme pour une pièce qui tourne, on sait si elle tombera sur pile ou face que lorsqu'elle est tombée. Par le mécanisme d'Intrication (Entanglement), les qubits dépendent les uns des autres, quelle que soit la distance. Cela permet de corréler des informations de manière non locale. Enfin, le Parallélisme Quantique permet, dans notre labyrinthe, de trouver la sortie comme un liquide qui se répand et parcourt les chemins de manière séquentielle.

Ces mécanismes démontrent qu'il s'agit là d'une rupture technologique, d'un changement de paradigme. Un ordinateur quantique n'a pas les mêmes fonctionnalités qu'un ordinateur classique et ne peut le remplacer, mais il permet de résoudre des problématiques complexes spécifiques. Ce qu'un supercalculateur actuel mettrait 10 000 ans à résoudre, une machine quantique mature pourrait potentiellement le traiter en quelques minutes. L'intégration du quantique dans la stratégie d'entreprise offre des leviers de croissance inédits, particulièrement dans les secteurs traitant des données massives ou des simulations complexes.

•Optimisation financière et logistique : Le quantique est particulièrement performant dans la résolution de problèmes combinatoires. Par exemple, l'optimisation de portefeuilles financiers en temps réel, en tenant compte de milliers de variables de marché, ou la gestion de chaînes d'approvisionnement mondiales, où le nombre de scénarios possibles explose, deviennent soudainement traitables à grande échelle. Pour les entreprises industrielles, les économies potentielles sur la logistique ou la planification de la maintenance prédictive pourraient se chiffrer en millions d'euros annuels.

•R&D et Sciences de la vie : La capacité à simuler des interactions moléculaires au niveau atomique, des mécanismes quantiques par essence, va accélérer de façon exponentielle la découverte de nouveaux médicaments et la création de matériaux innovants. A terme, la médecine personnalisée, et la réduction des émissions de Co2 par des processus chimiques alternatifs ou de nouveaux matériaux capables d'absorber le Co2 offrent des perspectives révolutionnaires.

•Intelligence Artificielle démultipliée : Le couplage de l'IA avec la capacité de

Documents sauvegardés

calcul de l'ordinateur quantique pourrait bien ouvrir de nouvelles perspectives, tout comme le "Quantum Machine Learning" permettra d'entraîner des modèles d'IA sur des jeux de données aujourd'hui inaccessibles. Si le quantique est une promesse, il porte en lui une menace technologique majeure : la fin de la cryptographie telle que nous la connaissons.

•La menace sur la cybersécurité : La plupart de nos protocoles de sécurité actuels (RSA, ECC) qui protègent nos banques, nos armées et nos données privées,reposent sur la difficulté de factoriser de grands nombres. Un ordinateur quantique suffisamment puissant (doté de l'algorithme de Shor) pourrait briser ces barrières et les rendre obsolètes. C'est ce qu'on appelle le "Q-Day".

•La menace est déjà avérée : c'est le "Harvest now, Decrypt later"» : Des acteurs malveillants ou étatiques interceptent et stockent dès aujourd'hui des données chiffrées sensibles (secrets industriels, données de santé, secrets d'État) dans l'intention de les déchiffrer dès que la technologie quantique sera disponible.

•Risque de dépendance technologique : La concentration des capacités quantiques entre les mains de quelques géants du cloud (États-Unis, Chine) pose un défi de souveraineté et de continuité d'exploitation pour les entreprises européennes.

•La Dynamique du "Premier Entrant" : L'avantage quantique est asymétrique. Dans des secteurs comme la pharmacie ou les matériaux, la première entreprise qui découvrira une nouvelle molécule grâce au quantique pourra la breveter et verrouiller la propriété intellectuelle. La gouvernance ne peut plus déléguer la question quantique à la seule direction technique (CTO). Elle doit s'emparer du sujet sous trois angles critiques : A. La révision de la stratégie à long terme Le conseil doit s'interroger : notre modèle d'affaires est-il exposé à une disruption quantique ? Un concurrent ou un nouvel entrant équipé de capacités quantiques peut-il remettre en cause nos avantages historiques (brevets, barrières à l'entrée, efficacité opérationnelle) ? Faut-il investir dans un partenariat avec des acteurs quantiques, suivre des projets pilotes, ou renforcer notre veille technologique ? Action : Inscrire le "Quantum Readiness" à l'ordre du jour des comités stratégiques et challenger la direction générale sur la préparation de scénarios. B. La surveillance du risque cyber (Post-Quantum Cryptography) Il est urgent d'exiger un audit de la résilience cryptographique. Quelles données sont réellement stratégiques ? Sont-elles chiffrées avec des protocoles susceptibles d'être cassés à moyen terme ? Où se trouvent les principaux risques d'exposition (chaîne de fournisseurs, cloud, partenaires...) ? Actions immédiates :

•Inventorier les actifs numériques et les données à forte valeur future (propriété intellectuelle, données de santé, contrats stratégiques).

•Initier le passage vers des protocoles de cryptographie post-quantique, en suivant les préconisations des autorités nationales et européennes.

•Exiger des fournisseurs critiques une feuille de route de compatibilité post-quantiqueC. La guerre des talents et l'éthique Le Conseil doit anticiper la nécessité de recruter, fidéliser ou former les experts quantiques et cybersécurité. Mais il doit aussi veiller à la qualité des décisions, en s'entourant d'experts externes indépendants pour éviter l'enfermement technologique ou la surpromesse des nouveaux acteurs. Sur le plan éthique, la gouvernance devra anticiper les impacts de l'utilisation du quantique sur la vie privée, l'équité des algorithmes ou la souveraineté des données. L'ordinateur quantique n'est pas une simple évolution technologique : il s'agit d'une rupture industrielle. Pour les conseils d'administration, le principal risque est l'attentisme. Un Conseil qui ignore le quantique aujourd'hui s'expose à l'obsolescence stratégique demain. La gouvernance moderne doit anticiper ces cycles technologiques longs. Pour cela, elle doit :

•Mettre en place une veille active sur les évolutions du quantique, en s'appuyant sur des réseaux spécialisés (CIGREF, European Quantum Industry Consortium, etc.) et des formations continues pour les administrateurs.

•Intégrer le quantique dans l'analyse de matérialité des risques et dans la cartographie stratégique de l'entreprise.

•Challenger régulièrement les plans d'action de la direction sur la sécurité des données et la robustesse des protocoles.

•S'impliquer dans les initiatives européennes de standardisation et de souveraineté numérique : le quantique ne sera maîtrisé que collectivement. L'ordinateur quantique ne relève pas de la simple évolution technologique : il marque une véritable rupture de civilisation industrielle. Face à ces cycles technologiques longs, la gouvernance moderne impose une anticipation sans faille. Pour les conseils d'administration,

Documents sauvegardés

l'heure n'est plus à l'observation mais à l'engagement, par l'intégration immédiate d'une feuille de route quantique au coeur de la stratégie. En pilotant activement cette mutation, les administrateurs transformeront ce défi en un levier de souveraineté et de maîtrise durable. À lire également : Les 10 technologies stratégiques pour 2026 selon Gartner

Documents sauvegardés

L'actualité

news·20260204·TUW·014

Nom de la source
L'Actualité (site web)

Type de source
Presse • Presse Web

Périodicité
En continu

Couverture géographique
Provinciale

Provenance
Montréal, Québec, Canada

Mercredi 4 février 2026

L'Actualité (site web) • 3703 mots

L'ordinateur de tous les dangers

Andrew Seale

L'informatique quantique et ses promesses de calculs à une vitesse inconcevable pousseront le monde numérique tel que nous le connaissons aujourd'hui, et par conséquent le concept de vie privée, au bord du précipice. Il ne reste qu'à savoir quand.

Un jour, quelqu'un, quelque part, disposera d'un ordinateur quantique capable de déchiffrer les codes fragiles qui sous-tendent toutes les données que nous échangeons sur Internet. On ne sait pas quand. Ce pourrait être dans 10 ans. Peut-être plus tôt. Mais les experts s'accordent à dire que le moment où nous basculerons dans l'ère quantique, communément appelé le « Jour Q », approche. Et notre version du monde pourrait s'effondrer -- les courriels envoyés, les secrets révélés via la fibre optique, les achats par carte de crédit, les résultats numérisés d'analyses médicales, les cryptages protégeant l'ordre soigneusement établi qui définit nos vies numériques.

Pour Gilles Brassard, cryptographe septuagénaire et professeur d'informatique à l'Université de Montréal, cette évolution va inverser le cours du temps. Si nous passons à la quantique demain, les données d'aujourd'hui seront perdues.

La quantique est une question de taille et d'efficacité. Les ordinateurs actuels abordent les problèmes étape par étape, mais les ordinateurs quantiques pourront théoriquement utiliser les principes de la mécanique quantique pour explorer simultanément de nombreuses possibilités, ce qui leur permettra de traiter des problèmes complexes, comme le décryptage d'un code, de manière exponentiellement plus rapide. Les pirates informatiques le savent. Ils ont commencé à s'y préparer en collectant et en stockant de grandes quantités de données afin de pouvoir les décrypter lorsqu'un ordinateur quantique sera disponible. Ce type d'attaque se définit ainsi : « moissonner aujourd'hui, déchiffrer plus tard ». « Terrifié... Je suis complètement terrifié », dit Gilles Brassard.

La terreur de Brassard a ceci de particulier qu'elle valide son travail. Car, dans un sens, c'est un avenir auquel il nous a préparés. Il y a plus de 40 ans, il a contribué à mettre au point l'une de nos meilleures défenses contre le futur postquantique : le protocole BB84, un moyen sophistiqué et incroyablement sûr de transférer des données cryptées à l'aide de la mécanique quantique. « Il a été mathématiquement prouvé que le protocole que nous avons inventé en 1983 est inconditionnellement sécurisé », explique Gilles Brassard... à condition que la théorie quantique soit juste et mise en oeuvre sans introduction de failles techniques ou de lacunes. En d'autres termes, BB84 fonctionne si la mécanique quantique, l'une des plus complexes et des plus belles théories sur les rouages de notre monde, est exacte.

Né à Montréal d'un père comptable et d'une mère prof de yoga, ayant grandi entouré de trois frères et d'une soeur, Gilles Brassard se révèle un prodige parmi les prodiges. Il fréquente l'Université de Montréal dès 13 ans (pour étudier les sciences ; deux ans plus tard, il s'inscrit au Département d'informatique), suivant les traces de son frère aîné, Robert, entré à l'université à 15 ans. « Il m'a enseigné toutes les mathématiques de niveau universitaire lorsque j'étais à l'école primaire », dit Gilles Brassard à propos de son frère.

En 1979, à l'âge de 24 ans, il obtient un doctorat en informatique théorique à l'Université Cornell. La même année, il assiste à un symposium à San Juan (Porto Rico), où il donne une conférence sur la cryptographie. Alors qu'il nage devant l'hôtel, un inconnu l'aborde dans l'eau.

Documents sauvegardés

« Il m'a affirmé qu'il savait comment utiliser la théorie quantique pour fabriquer des billets de banque impossibles à contrefaire », relate Gilles Brassard.

Cet inconnu est Charles H. Bennett, physicien américain qui deviendra l'autre « B » de BB84. À l'époque, Brassard ne s'intéresse absolument pas à la théorie quantique ni à la physique, mais là, flottant dans l'Atlantique, un peu captif, il écoute poliment.

L'idée que prêche Bennett vient de Stephen Wiesner, un physicien rencontré à l'Université Brandeis, au Massachusetts, dans les années 1960. « J'ai immédiatement remarqué une lacune importante », raconte Gilles Brassard, perpétuellement attiré par ce qui semble insoluble. « Les billets inventés par Wiesner ne pouvaient en théorie être contrefaits, mais leur validité ne pouvait être vérifiée par quiconque, à part les personnes qui les avaient fabriqués. »

L'article de Wiesner sur les billets de banque quantiques avait été rejeté par une revue d'ingénierie, sans doute en raison de son jargon de la physique, croit Gilles Brassard. Wiesner l'avait donc rangé dans un tiroir et était passé à autre chose. « Bennett, lui, avait compris que ça ne devait pas être abandonné, dit Brassard. Je ne sais pas à combien de personnes il a essayé d'en parler, mais aucune ne lui a prêté attention avant moi. »

À peine une heure après leur rencontre à San Juan, ils avaient élaboré un moyen de retravailler le système de billets de banque quantiques de Wiesner avec la cryptographie à clé publique. Cette technologie utilise une paire de clés numériques : l'une accessible à tout le monde pour crypter un message, et l'autre, gardée secrète, dont seul le destinataire peut se servir pour le décrypter. C'est comme une boîte aux lettres dans laquelle tout le monde peut déposer une missive, mais que seule la personne qui possède la clé peut ouvrir pour lire ce qu'elle contient.

Aujourd'hui, la cryptographie à clé publique est une fonction invisible de notre existence en ligne, qui intervient lorsque nous envoyons un courriel et chaque fois que nous accédons à un site Web dont l'adresse commence par « https ». Elle est essentielle, discrète, automatique, un peu comme la respiration ou le clignement des yeux. Mais en 1979, la cryptographie à clé publique est une nouvelle discipline, introduite trois ans plus tôt à l'Université Stanford par Martin Hellman et Whitfield Diffie, aidés par les travaux de Ralph Merkle à l'Université de Californie à Berkeley. Brassard et Bennett voient la possibilité d'utiliser la mécanique quantique pour reproduire ce que fait la cryptographie à clé publique, mais de manière plus sécurisée.

Pour comprendre minimalement la mécanique quantique, il faut accepter l'écart considérable entre ce que nous percevons comme vrai (en physique classique, une balle lâchée tombe immanquablement au sol) et l'absurdité de notre monde à l'échelle subatomique. Les électrons et les photons, particules sans masse ou presque sans masse transmises par fibre (photons) ou par l'air (électrons), peuvent parfois exister sous forme d'ondes ou se trouver à deux endroits à la fois. Ils peuvent s'entremêler, influençant immédiatement l'état de l'autre dans l'espace et le temps. Le fait d'observer ou de mesurer une particule peut modifier son comportement. Nous ne percevons pas ces choses : elles sont minuscules, invisibles et complètement en contradiction avec ce que nous savons du monde.

C'est cette incertitude du monde quantique que Bennett et Brassard veulent exploiter. Les deux forment une paire un peu particulière : l'un est cryptographe et l'autre est physicien, chacun mesurant la réalité à sa manière. Brassard enseigne l'informatique à l'Université de Montréal et Bennett est chercheur au centre de recherche d'IBM à Yorktown Heights, dans l'État de New York. Cet après-midi à San Juan sera suivi de plusieurs années d'allers-retours en avion et en voiture, pendant lesquelles les deux hommes vont rester en contact et poursuivre leur réflexion sur les points de convergence entre la physique quantique et la cryptographie, et sur la façon d'utiliser ces deux disciplines pour empêcher l'espionnage. « On a continué de se rendre visite », raconte Gilles Brassard.

À lire aussi

Votre aspirateur vous espionne-t-il ?

En 1983, Bennett et Brassard rédigent ensemble un article sur l'utilisation des effets quantiques pour sécuriser les communications. Leur idée est de crypter un message dans un signal quantique, de telle sorte que si un espion tente de l'intercepter et de mesurer les photons, ceux-ci seront perturbés de manière irréversible et détectable. Une façon ingénieuse d'utiliser la particularité quantique apparemment irrationnelle, selon laquelle le simple fait de mesurer ces minuscules particules (électrons, photons, atomes) modifie leur existence.

Mais il est extrêmement difficile d'envoyer un message sous forme de pho-

Documents sauvegardés

tons individuels par fibre optique sur une distance notable. « La plupart n'arrivent pas à destination, explique Gilles Brassard. Si Bob ne reçoit que 1 % du message, ce n'est pas très satisfaisant. »

Ils soumettent leur article à un congrès sur l'informatique. Il est refusé. Ils ont alors une autre idée : et si, au lieu d'envoyer le message lui-même, ils utilisaient un signal quantique pour transmettre une clé de chiffrement secrète à usage unique, impossible à intercepter sans qu'elle soit détectée ?

BB84 fait ses débuts officiels, sans grand retentissement, en 1984. « L'accueil général a été soit "c'est une jolie idée qui ne marchera pas", soit "ça n'a aucun bon sens" », raconte Gilles Brassard.

C'est ainsi que naît BB84, le premier protocole de cryptographie quantique pour la distribution de clés quantiques [connue sous le sigle anglais QKD]. BB84 fait ses débuts officiels, sans grand retentissement, à une conférence internationale sur les ordinateurs, les systèmes et le traitement du signal à Bangalore, en Inde, en 1984. « L'accueil général a été soit "c'est une jolie idée qui ne marchera pas", soit "ça n'a aucun bon sens" », raconte Gilles Brassard.

Bennett et Brassard construisent ensuite un prototype avec John Smolin, d'IBM Yorktown, et deux étudiants de Brassard, François Bessette et Louis Salvail. L'appareil a à peu près la longueur d'une table à manger. Fin octobre 1989, ils envoient la première transmission quantique secrète au monde. Elle ne parcourt que 32,5 cm, mais permet de prouver la validité du concept. Ils ont utilisé un prisme de Wollaston pour polariser les photons -- ce qui revient à les faire tourner à différents angles afin d'établir une clé de chiffrement. Le problème est que l'alimentation électrique qui sert à faire fonctionner l'appareil produit un bruit différent pour chaque polarisation, par conséquent un espion pourrait mémoriser les diverses tonalités et décoder la clé.

Cette expérience leur permet de publier un article dans Scientific American, ce qui élargit considérablement leur lectorat. On peut imaginer que cela ne vient pas sans un certain pincement : ce n'est pas leur belle théorie sur la QKD qui leur vaut cette reconnaissance pour BB84, mais un prototype gadget de QKD construit dans le laboratoire de quelqu'un d'autre.

Michele Mosca est aujourd'hui considéré comme un leader mondial à la croisée de l'informatique quantique et de la cryptographie. Il a créé plusieurs jeunes pousses, dont evolutionQ, qui aide les organisations à passer de pratiques et systèmes vulnérables à la cryptographie quantique à des pratiques et systèmes sécurisés. Mais en 1989, alors que Brassard et Bennett construisent le prototype BB84, Mosca est encore au secondaire, remportant des prix dans des concours de mathématiques.

Les maths, Mosca en mange. Élevé par des parents immigrés italiens dans une région rurale près de Windsor, en Ontario, il voit ses aptitudes lui valoir une bourse pour l'Université de Waterloo, où il s'intéresse à la cryptographie. À l'époque, les ordinateurs deviennent omniprésents et de plus en plus de données sont échangées sous forme numérique. Le monde a plus que jamais besoin de cryptage. Le chemin professionnel de Mosca semble tout tracé.

À lire aussi

La tragique histoire du premier ordinateur

Il fait la connaissance de Gilles Brassard à Crypto '94, une conférence sur la cryptographie à Santa Barbara, en Californie. « Je savais qu'il était une star », raconte Mosca. Il lui demande sur quoi il travaille. « C'était "quantique ci, quantique ça". Je me suis dit : "Wow, il y va vraiment à fond dans ce truc quantique." »

Lors de la même conférence, Michele Mosca s'entretient avec Don Coppersmith, un cryptographe et mathématicien qui travaille sur les algorithmes quantiques. Coppersmith lui explique comment un ordinateur quantique peut piéger des ions et les manipuler à l'aide de lasers (le piégeage des ions est un processus essentiel dans l'utilisation des qubits, les unités fondamentales d'information dans les ordinateurs quantiques). L'idée de bombarder des ions avec des lasers semble farfelue à Mosca. « Je pensais que Coppersmith plaisantait, raconte-t-il. J'ai même fait une remarque sarcastique du genre : "Où comptez-vous publier ça, dans le National Enquirer ?" »

En cette même année 1994, Peter Shor, un informaticien théoricien américain, met au point ce qui est désormais connu sous le nom d'algorithme de Shor, qui montre qu'un ordinateur quantique approprié sur le plan cryptographique, c'est-à-dire doté d'une puissance de calcul suffisante pour exécuter des algorithmes, ne prend pas toute la durée de vie de l'univers pour déchiffrer un code. En fait, il peut le faire de manière très efficace.

Peter Shor, Gilles Brassard et Charles H.

Documents sauvegardés

Bennett ont reçu le prix Breakthrough 2023, catégorie Physique fondamentale, des mains de l'actrice Kristen Bell et de l'astronaute Mae Jemison. (Photo : Tommaso Boddi / Breakthrough Prize / Getty Images)

Deux ans plus tard, Lov Grover, un informaticien, crée un algorithme capable de diminuer considérablement le nombre de cryptages qu'un pirate informatique devra essayer pour déchiffrer une clé cryptée privée. Cet algorithme réduit de moitié le niveau de sécurité des principales normes de cryptage, explique Atty Mashatan, directrice fondatrice du Laboratoire de recherche sur la cybersécurité de la Toronto Metropolitan University et membre du Conseil consultatif sur la quantique du Canada. L'algorithme de Shor représente une menace certaine. Selon Atty Mashatan, il renvoie carrément les cryptographes « à la case départ », même après 20 ans.

En 1995, Michele Mosca s'inscrit à l'Université d'Oxford pour sa maîtrise, continuant à travailler sur la création et le décryptage de codes à l'aide de la cryptographie classique. Il s'entête à demeurer dans les « si » : « si » nous construisons un ordinateur quantique, « si » nous pouvons atteindre la capacité de calcul avec ledit ordinateur... « si », « si », « si ». De son point de vue, l'informatique quantique ne peut exister dans le monde actuel.

Mais le propre de l'avenir est d'avoir une trajectoire changeante.

Le directeur de mémoire de Mosca, Dominic Welsh, un mathématicien britannique, lui présente Artur Ekert, un professeur de physique quantique, qui explore l'idée de la distribution de clés quantiques à l'aide de particules intriquées. Artur Ekert invite Michele Mosca à Turin pour lui faire connaître une petite communauté, en pleine expansion, de pionniers de l'informatique quantique. Cette rencontre suffit à le convaincre de l'inévitabilité de cette dernière. « J'ai compris que cela demanderait des décennies, mais que cela fonctionnerait », dit-il. Il est dès lors persuadé que quelqu'un dans ce groupe finira par construire un ordinateur quantique.

À lire aussi

L'informatique quantique, la prochaine fierté québécoise ?

Au cours de ses études de doctorat, toujours à Oxford, Michele Mosca recentre ses recherches sur les ordinateurs quantiques et la manière dont ils redéfinissent ce qui est sécurisé et ce qui ne l'est pas. En collaboration avec Gilles Brassard, Peter Høyer et Alain Tapp, Michele Mosca corédige un article très cité et désormais essentiel sur l'algorithme de Grover, qui contribue à cristalliser une partie de la menace quantique. L'article est publié en 2000.

En 2001, des chercheurs d'IBM et de l'Université Stanford collaborent pour mettre en oeuvre l'algorithme de Shor sur un processeur à sept qubits, soit une combinaison de molécules dans un tube à essai, chaque molécule étant un minuscule ordinateur quantique. Ce processeur informatique réussit à factoriser avec succès le nombre 15, un petit -- mais difficile -- problème mathématique. Cela constitue une avancée monumentale dans l'exécution d'un algorithme quantique et marque le début de la fin pour la cryptographie classique. Le grand « si » impossible n'est pas devenu « quand », mais « dans combien de temps ».

Des centres de recherche quantique commencent alors à voir le jour. En 2002, Michele Mosca et Raymond Laflamme (dont le directeur de thèse fut Stephen Hawking) s'associent à quelques autres personnes pour mettre sur pied l'Institut interdisciplinaire d'informatique quantique (IQC) de l'Université de Waterloo. Mike Lazaridis, le fondateur de Research in Motion, qui a créé le BlackBerry, s'implique. « Mike a annoncé qu'il donnerait un dollar pour chaque tranche de deux dollars que l'université allait injecter dans le projet », raconte Michele Mosca. L'investissement personnel de Lazaridis va dépasser les 100 millions de dollars, ce qui permettra au groupe quantique de collecter des fonds et de commencer les embauches.

Il faudra près d'une quinzaine d'années pour que la prise de conscience de la menace quantique fasse une percée décisive. En 2015, l'Agence nationale de la sécurité des États-Unis (NSA), spécialisée dans le renseignement d'origine électromagnétique et la cybersécurité, déclare qu'elle passe à la cryptographie à résistance quantique. À peu près à la même époque, Michele Mosca, Atty Mashatan et Ken Giuliani, consultant en cryptographie auprès de la Banque CIBC, contribuent à la création d'un groupe de travail sur la quantique afin d'évaluer la menace que représente cette technologie pour le secteur financier.

Cette équipe devient le Groupe de travail sur la préparation en matière de technologie quantique, qui travaille sous l'égide du Forum canadien pour la résilience des infrastructures numériques, dont les membres comprennent Google, Accenture, Amazon

Documents sauvegardés

Web Services (AWS) et BlackBerry, ainsi que des acteurs clés des infrastructures critiques tels que les principales institutions financières canadiennes, l'Autorité ontarienne de réglementation des services financiers et la Banque du Canada. De 2020 à 2024, il publie un guide annuel des pratiques exemplaires en matière de préparation à l'ère quantique.

Un des ordinateurs quantiques de Google au laboratoire de l'entreprise à Santa Barbara, en Californie. (Photo : Google)

En 2024, l'Institut national des normes et de la technologie (NIST), une agence fédérale américaine qui joue un rôle central dans l'établissement des directives en matière de cybersécurité et de cryptage, publie la première version complète de ses normes de cryptographie postquantique. Elles sont résistantes à la technologie quantique et conçues pour fonctionner sur des ordinateurs traditionnels. « Elles ne sont pas infaillibles à 100 %, précise Atty Mashatan. Nous pensons qu'elles résisteront à la puissance d'un ordinateur quantique, [mais] nous ne disposons pas d'un [tel ordinateur pour le moment]. »

En janvier 2025, l'Agence spatiale canadienne a annoncé qu'elle accordait plus de 1,4 million de dollars à QEYnet -- une jeune pousse spécialisée dans les communications quantiques établie à Maple, en Ontario -- pour qu'elle installe sa charge utile de transmission de photons, de la taille d'un carton de lait, sur un satellite de la grosseur d'un four à micro-ondes, puis qu'elle le lance dans l'espace. Cette technologie utilise la QKD pour transmettre des codes de cryptage entre les satellites et les stations au sol. Le lancement du satellite doit avoir lieu au cours de l'année [il a été reporté à 2026]. « Nous intégrons le protocole BB84 dans notre matériel », explique Cordell Grant, PDG de QEYnet.

Ce ne sera pas la première fois que le protocole BB84 sera utilisé dans l'espace. En 2016, la Chine a envoyé un microsatellite quantique pour tester la QKD et l'intrication quantique sur de longues distances, et a ainsi réussi à créer une clé secrète entre la Chine et l'Autriche l'année suivante. Mais les ambitions de QEYnet sont plus larges : l'entreprise souhaite mettre la QKD à la portée d'un plus grand nombre. « Nous essayons de la commercialiser », dit Cordell Grant.

Des projets tels que QEYnet soulèvent également une question : comment établir notre hiérarchie des secrets, et lesquels méritent d'être protégés par l'envoi de photons depuis des satellites ?

Le prototype de QEYnet est un bond en avant par rapport à l'invention BB84 de Brassard et Bennett, qui en 1989 produisait le bourdonnement typique des appareils à haut voltage. Il est par ailleurs très technique. D'abord, le dispositif de transmission QKD doit être petit afin de ne pas surcharger le satellite. Mais il doit tout de même être capable de recevoir un photon émis à des centaines de kilomètres de distance.

Cette technologie a plusieurs applications. Elle peut faciliter les communications sécurisées par cryptage quantique avec des satellites cartographiant des données en temps réel sur un champ de bataille, par exemple. Elle peut également être utilisée pour protéger les données de charge utile des satellites contre les satellites eux-mêmes. Après tout, ceux-ci sont souvent lancés par des sociétés spatiales tierces.

Les projets tels que celui de QEYnet représentent les limites actuelles de la technologie QKD, tant sur le plan physique que du point de vue technique. Ils soulèvent également une question : comment établir notre hiérarchie des secrets, et lesquels méritent d'être protégés par l'envoi de photons depuis des satellites ?

À lire aussi

Satellites : comment mieux gérer le far west spatial ?

Dans les décennies qui ont précédé la mise au point du protocole BB84 par Brassard et Bennett, l'échange de secrets avait une signification différente. Ils étaient troqués par des espions et des chefs d'État, les clés de décryptage étant souvent transmises clandestinement au prix d'efforts considérables. Aujourd'hui, nous livrons des secrets dès que nous tenons nos écrans lumineux entre nos mains et envoyons un texto ou un courriel. Peu importe le secret, qu'il s'agisse d'informations bancaires ou d'un mème, il est protégé et, dans la plupart des cas, toujours indéchiffrable.

Jusqu'à ce que tout s'écroule.

Gilles Brassard ne veut pas qu'on lui demande dans combien de temps arrivera l'ordinateur quantique. La réponse ne serait que supposition de toute façon. Encore une fois, personne ne sait exactement quand nous disposerons de cette technologie. « Mais elle s'en vient, dit-il, il n'y a plus d'obstacles majeurs. »

De son point de vue, le mal est déjà fait. Le nombre croissant de vols de données nous montre bien que notre identité, nos propos et nos actes sont exposés

Documents sauvegardés

au grand jour, autant d'infos stockées dans des archives malveillantes en vue d'une exploitation future. « On ne peut rien faire pour sauver le passé », dit Gilles Brassard. Mais il y a quelques solutions. Il nous suffit d'attendre que l'inconnu se dévoile pour voir si elles fonctionnent.

« Cette incertitude existera toujours », croit Atty Mashatan. Nous vivons avec elle. Alors que nous nous dirigeons à toute vitesse vers le Jour Q, nous l'acceptons. L'être humain est incapable de résister à l'envie de rechercher toujours plus de puissance -- des ordinateurs plus impressionnants sur nos bureaux, dans nos mains -- tout en sachant que cette puissance pourrait, entre de mauvaises mains, tout détruire. Comme le dit Atty Mashatan, nous ne pourrons probablement jamais empêcher complètement l'informatique quantique de déchiffrer nos codes. « Notre seul espoir est de rendre cette tâche plus difficile. »

La version originale de cet article est parue dans le magazine The Walrus.

.post-%%id%% { --font-custom: "Cutive Mono", var(--font-monospace), monospace; }.post-%%id%% figcaption { font-family: var(--font-custom); font-size:.8rem; word-spacing: -.1em; letter-spacing: -.005em; color: var(--color-text); }.post-%%id%%.wp-block-pullquote blockquote p { font-family: var(--font-custom); font-weight: bold; word-spacing: -.1em; letter-spacing: -.005em; text-transform: uppercase; }.post-%%id%%.first-line:first-line { font-family: var(--font-custom); font-weight: bold; font-size: 1.25em; line-height: 1.25; word-spacing: -.1em; letter-spacing: -.005em; }

Cet article est paru dans L'Actualité

(site web)

https://lactualite.com/techno/lordinateur-de-tous-les-dangers

Documents sauvegardés

Nom de la source
L'Union (France)
Type de source
Presse • Journaux
Périodicité
Quotidien
Couverture géographique
Régionale
Provenance
Reims, Grand Est, France

Dimanche 18 janvier 2026

L'Union (France)

• p. VIT10

• 529 mots

La révolution quantique à portée de tous au théâtre

Saint-Dizier. Les 19 et 20 janvier, le théâtre de Saint-Dizier accueille « Grand Est Quantique », deux journées de conférences et de spectacle pour comprendre une révolution scientifique majeure qui transforme déjà notre quotidien et façonne le monde de demain.

Les 19 et 20 janvier, le théâtre de Saint-Dizier accueillera « Grand Est Quantique », deux journées pour plonger au cœur d'une révolution scientifique qui bouleverse déjà notre quotidien et promet de transformer en profondeur les sociétés de demain. Smartphones, GPS, imagerie médicale, lasers ou nucléaire reposent déjà sur les lois de la physique quantique. Mais, comme le rappellent les chercheurs, nous n'en sommes qu'aux prémices d'un changement d'ampleur comparable à celui du nucléaire au XX e siècle ou du numérique à la fin du siècle dernier.

Pour guider le public dans ce monde de l'infiniment petit, la Ville de Saint-Dizier et ses partenaires ont fait appel à Charles-Antoine, physicien et enseignant-chercheur en physique quantique à Sorbonne Université, nommé ambassadeur de la médiation scientifique du Centre national de la recherche scientifique (CNRS) dans le cadre de l'année du centenaire de la physique quantique. Chercheur reconnu, il est aussi un pédagogue passionné, convaincu que la compréhension des grandes mutations scientifiques doit être partagée avec le plus grand nombre.

Lundi 19 janvier, il proposera deux conférences – l'une réservée aux lycéens, l'autre ouverte au grand public – pour expliquer ce qu'est réellement la physique quantique, ses principes fondateurs, ses promesses mais aussi ses enjeux économiques et géostratégiques. Il y sera question de superposition des états, de particules capables d'être « ici et ailleurs » en même temps, de calculs parallèles inimaginables dans l'informatique classique, et des perspectives offertes par les ordinateurs quantiques, appelés à révolutionner la cryptographie, les télécommunications, la conception de nouveaux matériaux ou encore la performance des capteurs.

Le mardi, après une conférence destinée spécifiquement aux militaires de la base 113, place à une forme originale de transmission avec le -spectacle « Equiquanto », imaginée avec le peintre Paul Kichilov. Devant le public, sous l'œil des caméras, l'artiste dessine en direct tandis que le scientifique raconte et explique. Le cheval devient alors le médiateur poétique de la pensée quantique. Animal à la fois lourd et aérien, doux et sauvage, rassurant et inquiétant, il incarne ces contradictions apparentes qui sont au cœur du monde quantique, où une particule peut se trouver dans plusieurs états simultanément. Pour Charles-Antoine, l'art permet de rendre sensible ce qui défie notre intuition : la superposition des possibles, impensable à notre échelle mais réelle à l'échelle quantique.

Charles Antoine rend la physique quantique (presque) compréhensible par tous.
. *CAP*

Un spectacle vu déjà

par 30 000 spectateurs

Ce spectacle, déjà vu par plus de trente mille spectateurs à travers la France, mêle rigueur scientifique et puissance évocatrice des images pour faire comprendre une révolution en marche, suivie de près par les États, les grandes puissances industrielles, les géants du numérique et un foisonnement de start-up.

Deux soirées pour découvrir, comprendre et s'émerveiller, au moment où la physique quantique s'apprête à franchir le seuil des laboratoires pour transformer le monde réel.

Documents sauvegardés

Documents sauvegardés

Nom de la source
IT for Business (site web)
Type de source
Presse • Presse Web
Périodicité
En continu
Couverture géographique
Nationale
Provenance
Paris, Ile-de-France, France

Mardi 27 janvier 2026

IT for Business (site web) •
1735 mots

L'accord entre C12 et Classiq rapproche le hardware quantique de l'usage pratique

Laurent Delattre

Par Laurent Delattre , publié le 27 janvier 2026 C12 et Classiq annoncent un partenariat pensé pour « renforcer les synergies entre matériel

et logiciel quantiques » et, surtout, rendre la R&D plus praticable dès maintenant, alors même que le quantique “utile” reste un horizon à construire.

La France n'a pas attendu que les ordinateurs quantiques sortent des laboratoires pour structurer un écosystème. Stratégie nationale, financements, industriels partenaires, start-up deeptech très visibles à l'international. L'hexagone s'est imposé parmi les places fortes mondiales du quantique, avec l'ambition affichée d'en faire une filière stratégique.

Et quand on parle des acteurs nationaux “qui comptent” côté deeptech quantique, un noyau revient systématiquement dans les discussions : Pasqal (et ses qubits d'atomes neutres), Quandela (et ses qubits photoniques), Alice & Bob (et ses qubits de chat)… et C12. Ce dernier s'est imposé dans le paysage avec une promesse (et une ambition) très particulière : développer dès le départ un ordinateur quantique universel qui passe réellement à l'échelle, avec correction d'erreurs, autrement une machine FTQC , là où tous les acteurs du marché ont plutôt cherché à expérimenter sur les très imparfaites machines NISQ. Fondée à Paris et issue des laboratoires de l'École Normale Supérieure et du CNRS, C12 travaille sur une technologie quantique basée sur les qubits de spin réalisés au sein de nanotubes de carbone ultra-purs (et mille fois plus fins qu'un cheveu), une approche matérielle radicalement différente des qubits supraconducteurs ou ioniques. C'est aujourd'hui l'une des architectures les plus prometteuses pour réduire le bruit et améliorer la fidélité des qubits.

L'intérêt de son approche est non seulement lié à la qualité et donc la fiabilité des qubits mais également au fait qu'elle doit permettre une industrialisation rapide et la création de machines quantiques très compactes. Pierre Desjardins, CEO & cofondateur de C12, résume l'axe directeur sans détour : « on est focalisé sur le fait de faire des ordinateurs quantiques qui marchent à grande échelle, qui intègrent dès le départ de la correction d'erreurs et aussi qui sont compacts. C'est la clé pour les voir un jour être déployés, notamment dans des datacenters d'entreprises. » C'est d'autant plus important que l'on voit mal pour le moment des ordinateurs quantiques isolés dans leur propre bulle. Ils joueront plutôt le rôle d'accélérateur. « C'est pourquoi C12 imagine des ordinateurs quantiques qui soient vraiment intégrés sur des datacenters et en connexion avec d'autres moyens de calcul, que ce soit des CPU ou des GPU, » confirme le CEO.

Cette insistance sur l'industrialisation n'est pas qu'un élément de langage. Il traduit une volonté de départ et une philosophie de design. Même si l'aventure n'en est qu'à ses débuts avec des QPU protos bien enfermés dans ses labos. « Aujourd'hui, il n'y a pas d'ordinateur quantique C12, même prototype, qui ait été livré à des clients. La seule date qu'on annonce, quant à une disponibilité, c'est à l'horizon 2033. » Mais la jeune pousse française devrait officialiser une roadmap plus précise dans le courant de l'année.

L'originalité C12 : la pureté du carbone pour des qubits fiables

Documents sauvegardés

L'approche revendiquée par C12 part d'un diagnostic simple : sans qubits de très haute qualité, les promesses de passage à l'échelle se heurtent vite au mur du bruit et des erreurs. D'où un choix technologique centré sur le matériau. C12 met en avant des processeurs reposant sur des nanotubes de carbone, « le matériau le plus pur », pour « minimiser drastiquement les erreurs quantiques », avec à la clé « une cohérence record et un faible niveau de bruit ». Et Pierre Desjardins de confirmer :

« C12 construit des technologies capables de passer à l'échelle avec des qubits de très haute qualité, parce qu'à un moment le besoin de qualité est forcément clé quand on veut faire passer à l'échelle. C'est aussi pour ça qu'on voit que des approches qui existent aujourd'hui ont de plus en plus de mal à augmenter le nombre de qubits : elles sont limitées par la qualité de leurs qubits. »

Techniquement, C12 travaille sur des qubits de spin d'électron, piégés dans un nanotube de carbone, comme une sorte de “transistor quantique” extrêmement petit.

Autre argument clé : la compatibilité avec les filières industrielles existantes. Pour C12, le passage à l'échelle doit pouvoir s'appuyer sur l'outillage et les savoir-faire de l'industrie des semi-conducteurs.

Sans logiciel quantique, pas d'informatique quantique

Mais C12 a pleinement conscience que le hardware n'est qu'une partie de l'équation de l'informatique quantique. Cette informatique d'un nouveau genre impose en réalité de réinventer toute la stack informatique, du QPU jusqu'aux applications en passant par les algorithmes, les bibliothèques, les outils de développement, les compilateurs.

C'est là que le partenariat avec Classiq annoncé aujourd'hui prend tout son sens. L'informatique quantique ne se résume pas à empiler des qubits. Elle impose une refonte de la chaîne complète, depuis l'expression du problème jusqu'à sa traduction en circuits exécutables sur un matériel donné.

Entreprise israélienne basée à Tel Aviv, « Classiq, c'est une entreprise qui a développé une plateforme pour les chercheurs, développeurs et mathématiciens qui cherchent à développer dès aujourd'hui des programmes pour les ordinateurs quantiques » résume Simon Fried, VP Corporate Communications chez Classiq. « C'est une solution conçue pour permettre aux gens de créer des circuits quantiques beaucoup plus avancés, beaucoup plus facilement, beaucoup rapidement, avec un langage qui est très abstrait. »

L'algorithmique quantique est un univers de recherche à part entière. Les algorithmes eux-mêmes obéissent à des logiques contre-intuitives, exploitant des phénomènes comme la superposition et l'intrication quantique.

« En informatique classique, on fait beaucoup de ‘design patterns'. On prend des morceaux et on les combine. Par contre, sur le quantique, ce n'est pas vraiment comme ça, que cela fonctionne. Ne serait-ce que parce que le nombre d'algorithmes quantiques est vraiment assez limité. Aujourd'hui, on parle de centaines ou de milliers, c'est tout. Là où l'informatique classique est plutôt bâtie sur une infinité d'algorithmes. »

Cette relative rareté des algorithmes quantiques s'explique par la difficulté fondamentale à concevoir des programmes qui exploitent réellement l'avantage quantique. Comme le souligne Simon Fried, « il y a un nombre relativement limité de choses qui peuvent vraiment bénéficier des ordinateurs quantiques ». Pour autant, dans ces domaines spécifiques, comme la simulation moléculaire, l'optimisation combinatoire ou la cryptographie, les gains potentiels sont considérables.

Pourquoi l'approche Classiq “a le vent en poupe”

Classiq s'est positionné sur un chaînon manquant de la stack quantique actuelle : une plateforme qui permet de décrire un problème à un haut niveau d'abstraction (y compris en langage naturel via l'IA conversationnelle), puis de laisser une chaîne de compilation/synthèse produire un circuit optimisé, en fonction des contraintes et de la cible matérielle.

Face à la complexité de la programmation quantique, l'approche de Classiq consiste donc à élever le niveau d'abstraction pour simplifier et universaliser le développement quantique. Plutôt que de demander aux développeurs de manipuler directement les portes quantiques et les circuits, la plateforme leur permet de travailler au niveau du modèle mathématique.

« Quand on utilise un kit de développement comme le populaire Qiskit d'IBM, on doit dès le départ penser aux portes quantiques de l'ordinateur, et elles sont différentes dans tous les ordinateurs quantiques qui existent aujourd'hui » déchiffre Simon Fried. « Nous, on sépare ces deux phases. Le développeur se focalise sur les questions de « c'est quoi

Documents sauvegardés

le problème » et « comment l'exprimer mathématiquement ». Et notre outillage prend automatiquement en charge la deuxième phase : un mécanisme de transpilation prend ce modèle et en fait un circuit quantique adapté au hardware visé. »

Cette séparation entre modèle et implémentation est cruciale. Car les machines quantiques actuelles sont toutes différentes : supraconducteurs chez IBM, ions piégés chez IonQ, atomes neutres chez Pasqal, photons chez Quandela, nanotubes de carbone chez C12. Chaque technologie a ses propres contraintes, ses propres portes natives, ses propres topologies de connexion entre qubits.

L'intérêt d'une plateforme comme Classiq est aussi économique. Car le temps de calcul sur un ordinateur quantique coûte cher, et un circuit mal optimisé peut multiplier les coûts par dix ou cent. La capacité à générer automatiquement des circuits optimisés pour chaque matériel devient un avantage compétitif majeur.

Callisto, le jumeau numérique de C12, arrive dans Classiq

Concrètement, le partenariat entre C12 et Classiq se matérialise par l'intégration de Callisto, l'émulateur quantique de C12, dans la plateforme Classiq. Callisto est capable de simuler jusqu'à 13 qubits en reproduisant fidèlement les caractéristiques physiques et le bruit réel de l'architecture à nanotubes de carbone. « L'émulateur Callisto a un modèle de bruit qui est vraiment réaliste, qui est vraiment basé sur ce qu'il y a au niveau physique. Ce qui est intéressant quand on va tester un algorithme dessus, c'est qu'on a vraiment une idée assez précise du fonctionnement sur le hardware réel de C12 » précise Pierre Desjardins.

Les développeurs peuvent désormais utiliser le langage Qmod et le moteur de synthèse de Classiq pour concevoir, compiler et tester leurs algorithmes sur Callisto. Une manière de préparer dès aujourd'hui les applications qui tourneront demain sur les véritables processeurs quantiques de C12. « L'outil Classiq, c'est un peu comme le WordPress du quantique. C'est très intuitif. Ça permet à des gens pour qui le quantique n'est pas forcément suffisamment stratégique pour avoir des projets dédiés, de commencer à tester des choses, des workflows, explorer des petits algorithmes. »

Une étape clé pour “déverrouiller” l'adoption

Pourquoi une telle annonce maintenant ? Pour trois raisons. D'abord, s'inscrire au plus tôt dans des logiques d'intégration entre hardware et software.

Ensuite, valider techniquement la compatibilité entre un matériel conçu pour le passage à l'échelle (C12) et un logiciel pensé dans la même optique (Classiq).

Enfin, gagner en visibilité auprès de cette communauté croissante de chercheurs, étudiants, développeurs, industriels qui se passionnent déjà pour les développements quantiques. Car comme le rappelle Simon Fried, « il est très facile avec l'outil Classiq de faire des comparaisons entre hardware… Or les entreprises se montrent d'ores et déjà très intéressées de pouvoir explorer différentes façons d'exécuter leurs algorithmes, comprendre mieux les implémentations hardware et explorer sur quelles technologies elles devraient investir leur temps. »

Au fond, ce partenariat C12 – Classiq vient rappeler que le quantique ne se jouera pas seulement sur une bataille de qubits. Il se jouera sur l'art de relier une R&D matérielle encore mouvante à une couche logicielle capable d'absorber le changement, de capitaliser sur un socle algorithmique limité mais puissant, et de transformer l'expérimentation en ingénierie. « Nous sommes convaincus que l'informatique quantique doit désormais résoudre de vrais problèmes industriels, pas seulement des défis théoriques », résume Pierre Desjardins. L'accord avec Classiq permet ainsi à C12 d'accélérer dans cette voie.

Cet article est paru dans IT for Business (site web)

https://www.itforbusiness.fr/laccord-entre-c12-et-classiq-rapproche-le-hardware-quantique-de-lusage-pratique-99701

Documents sauvegardés

news·20260115·CCMD·1000077_10541910859_100

Nom de la source
Le Journal du Net (JDN) (site web) - Le Journal du Net

Type de source
Presse • Presse Web

Périodicité
En continu

Couverture géographique
Nationale

Provenance
Paris, Ile-de-France, France

Jeudi 15 janvier 2026

Le Journal du Net (JDN) (site web) - Le Journal du Net • 717 mots

Cryptographie post-quantique : l'urgence d'un monde à sécuriser avant le Q-Day

Chronique de Laëtitia Berché

La cryptographie est au cœur de la confiance numérique. Pourtant, cette fondation est menacée par un horizon technologique inédit : l'arrivée des ordinateurs quantiques.

Ces machines, qui pourraient voir le jour entre 2030 et la fin du siècle (le spectre est large !), promettent une puissance de calcul telle qu'elles rendraient obsolètes les systèmes de chiffrement actuels. Une échéance connue sous le nom de Q-Day, date à laquelle les algorithmes de sécurité utilisés aujourd'hui ne résisteront plus.

Technologie quantique : une révolution scientifique et technologique

L'informatique quantique n'est pas un "big bang" immédiat, mais un chemin de longue haleine. Les premiers prototypes étaient encore de la science-fiction il y a dix ans. Aujourd'hui, plusieurs startups et laboratoires dont une quarantaine en Europe travaillent à industrialiser les technologies quantiques, qu'il s'agisse de simulateurs ou d'ordinateurs quantiques.

Comme le résument certains experts, l'émergence de ces machines serait l'équivalent de marcher sur la Lune. Elle nécessite un matériel spécifique, des décennies de recherche et une approche radicalement différente de l'informatique classique. Mais si cette promesse devient réalité, tout ce qui est chiffré aujourd'hui pourrait être déchiffré demain.

PQC – Une menace déjà présente : "collect now, decrypt later"

Le risque est d'autant plus sérieux que des attaquants peuvent dès aujourd'hui intercepter et stocker des données sensibles dans l'attente de pouvoir les déchiffrer demain. Ce principe du "prélever maintenant, déchiffrer plus tard" rend vulnérables toutes les informations qui conserveront une valeur stratégique dans 10 ou 15 ans : données de santé, brevets industriels, secrets d'État, transactions financières…

C'est pourquoi l'ANSSI appelle les organisations à considérer le passage à la cryptographie post-quantique (PQC) comme une priorité absolue, à engager dès maintenant.

Chiffrement post-quantique : une transition titanesque pour les entreprises

Passer au PQC ne se résume pas à changer un algorithme. Pour les organisations, le chantier est massif. Il va du fait d'auditer et inventorier l'ensemble des données et systèmes et flux qui reposent sur la cryptographie à mettre à jour les politiques de sécurité et les mécanismes d'authentification en passant par la formation et sensibilisation des équipes techniques et métiers et de la définition d'une feuille de route réaliste, budgétée et évolutive.

Un effort qui concerne en priorité les OIV (opérateurs d'importance vitale) et les OSE (opérateurs de services essentiels), mais qui finira par toucher toutes les entreprises. Or, à ce jour, seul un quart des RSSI prend réellement le sujet au sérieux.

Course au quantique : le rôle de l'État et la dynamique européenne

La puissance publique a commencé à structurer la réponse avec des textes comme NIS2 ou DORA, qui renforcent les obligations de résilience et d'encadrement. L'Europe, avec la France en pointe, dispose d'un tissu d'acteurs académiques et industriels capables de peser dans la course au quantique. Reste

Documents sauvegardés

à savoir si cette dynamique permettra de bâtir une stratégie unifiée et de positionner l'UE comme un leader mondial.

Au-delà des technologies, c'est une question de souveraineté et de confiance. La cryptographie n'est pas qu'une brique technique : c'est le socle sur lequel repose la sécurité numérique de toute société.

Internet post-quantique : se préparer à l'inconnu

La difficulté est qu'aucune certitude n'existe encore : nul ne sait si, ni quand, un ordinateur quantique capable de casser les algorithmes actuels verra réellement le jour. Mais attendre serait une erreur stratégique.

Le défi est donc de se préparer à une menace hypothétique mais plausible, en posant dès aujourd'hui les fondations d'un Internet post-quantique.

Cela passe par une veille technologique continue, l'expérimentation de solutions hybrides de transition mais aussi le développement de nouvelles compétences au sein des entreprises et du monde académique, ou encore la mise en place d'une économie de services autour du quantique, qui accompagnera les grandes organisations dans ce virage.

Le Q-Day est ainsi une menace encore hypothétique mais trop sérieuse pour être ignorée. Comme pour d'autres ruptures technologiques, il ne s'agit pas d'attendre la révolution, mais de se préparer méthodiquement à l'affronter.

Le passage à la cryptographie post-quantique sera long, coûteux et complexe, mais il constitue le prix de la confiance numérique de demain.

Cet article est paru dans Le Journal du Net (JDN) (site web) - Le Journal du Net

https://www.journaldunet.com/cybersecurite/1547231-cryptographie-post-quantique-l-urgence-d-un-monde-a-securiser-avant-le-q-day/