Documents sauvegardés

Mardi 11 novembre 2025 à 15 h 33

7 documents

Sommaire

Documents sauvegardés • 7 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

Monday, October 27, 2025

Forbes (France) (site web) - Forbes.fr • 1328 mots

news·20251027·LUEM·214632_58034280124

LexisNexis

Le temps presse pour la sécurité de l'IA à l'ère de l'informatique quantique

Forbes

Catégorie : TechnologieL'IA est désormais présente dans les tribunaux, les hôpitaux, les aéroports, les banques et plusieurs secteurs industriels, devenant ainsi le fleuron de nombreuses entreprises modernes. Cependant, la protection de ces systèmes d'IA à l'ère de l'informatique quantique devient de plus en plus difficile. Entre l'optimisme suscité par l'IA générative et l'accélération de l'informatique quantique, il existe un risque croissant auquel peu d'entreprises s'intéressent aujourd'hui. Si beaucoup s'inquiètent des invites adversaires et des hallucinations des modèles, les experts affirment que ce ne sont là que des problèmes mineurs. David Harding, PDG d'Entrokey Labs, une entreprise de cybersécurité qui développe une infrastructure de clés résistante au quantique, a averti que le véritable risque réside dans la manière dont les systèmes d'IA traitent les données sensibles. Il a fait valoir que les systèmes d'IA, et les volumes massifs de données sensibles qu'ils ingèrent, pourraient bientôt être les premières victimes des cyberattaques quantiques. Et la plupart des entreprises avancent à l'aveugle vers cet avenir. Au début de l'année, Jensen Huang, PDG de Nvidia, a décrit l'informatique quantique comme ayant atteint « un point d'inflexion ». Si cette déclaration a suscité l'intérêt des investisseurs, ses implications pour la cybersécurité, en particulier pour les systèmes basés sur l'IA, n'ont pas encore été pleinement comprises.

À mesure que les chercheurs se rapprochent de la construction de machines quantiques évolutives, les protocoles de cryptage établis de longue date, tels que RSA et ECC, pourraient être piratés, rendant ainsi accessibles des données auparavant sécurisées. En d'autres termes, les données qui alimentent votre IA aujourd'hui pourraient constituer demain votre plus grande vulnérabilité. Il ne s'agit pas d'un scénario de science-fiction lointain. Les bases sont déjà jetées. On pense que des acteurs étatiques stockent des données cryptées selon une stratégie dite « collecter maintenant, décrypter plus tard ». Imaginez des voleurs qui dérobent aujourd'hui des coffres-forts verrouillés en sachant qu'ils auront les clés demain. Une fois que les machines quantiques seront suffisamment puissantes, elles pourraient décrypter rétroactivement des trésors de secrets d'entreprise, de communications militaires et de données médicales, y compris tout ce qui passe aujourd'hui par les modèles d'IA. « Toutes les données électroniques sont exposées au risque d'être collectées maintenant et décryptées plus tard si elles n'utilisent pas de clés numériques résistantes aux attaques IA actuelles et aux attaques quantiques à court terme », explique David Harding. « Plusieurs pays, dont la Russie, la Chine, l'Iran et la Corée du Nord, comptent plus de 100 000 personnes qui se consacrent exclusivement au piratage de nos systèmes. Ajoutez à cela l'automatisation, et l'ampleur du phénomène devient presque ingérable. » Le quantique menace tous les systèmes numériques, mais l'IA amplifie le risque. Ces modèles ne se contentent pas de générer du contenu, ils ingèrent des

Documents sauvegardés

dossiers médicaux, des modèles financiers, des données de propriété intellectuelle et des données juridiques. Dans les systèmes autonomes, ils prennent des décisions. Dans d'autres, ils écrivent du code et déclenchent des flux de travail. Cela place l'ensemble des pipelines d'IA, des données d'entraînement aux agents déployés, directement dans la ligne de mire. « Le cryptage quantique et sécurisé par l'IA a la même importance que les fondations d'un bâtiment », explique Scott Streit, directeur scientifique chez Entrokey Labs. « Sans lui, la structure s'effondre. Les données des clients, la propriété intellectuelle et les communications ne seraient plus protégées. En matière de sécurité nationale, les satellites ou les armes de précision pourraient être pris d'assaut. » Malgré ces risques, de nombreuses entreprises considèrent encore l'informatique quantique comme un problème futur, à résoudre d'ici 2030. L'Institut national américain des normes et technologies (NIST) a défini une feuille de route pour l'adoption d'une cryptographie quantique sécurisée d'ici 2035. Cependant, selon David Harding, ce calendrier ne reflète plus la vitesse à laquelle évoluent l'IA et les capacités quantiques. « Le calendrier est de plus en plus en décalage avec le rythme des progrès de l'IA et de l'informatique quantique », a déclaré David Harding. « Certains pensent que l'IA est déjà en train de s'introduire dans les systèmes de cryptage. » Et pourtant, la plupart des entreprises continuent de considérer la préparation à l'informatique quantique comme un projet informatique à long terme, nécessitant des années de consultations, de mises à niveau des infrastructures et d'évaluation des fournisseurs. David Harding qualifie cette attitude de « cyber-inertie », une stratégie dépassée face à une menace beaucoup plus rapide. « Nous essayons de résoudre une menace plus intelligente avec des réponses obsolètes », a déclaré David Harding. Scott Streit a ajouté que « l'IA est déjà capable de créer des mathématiques que les meilleurs mathématiciens ne peuvent expliquer », arguant que « la seule façon de gagner est d'utiliser l'IA pour sécuriser l'IA ». Pour aggraver les choses, les cadres réglementaires ne sont pas à la hauteur. Ni la loi européenne sur l'IA ni le cadre de gestion des risques liés à l'IA du NIST ne disent grand-chose sur la défense des systèmes d'IA contre les menaces cryptographiques quantiques, laissant ainsi une vulnérabilité critique sans réponse au niveau politique. Les conséquences financières d'une violation causée par le décryptage quantique sont difficiles à estimer. Toutefois, le principe est simple : ce qui est considéré comme sûr aujourd'hui ne le sera peut-être plus demain. Cela inclut les résultats confidentiels des modèles, les invites internes, les décisions enregistrées des agents et les métadonnées sensibles. Tout cela pourrait être exposé ou altéré. « Pensez à la façon dont nous réagissons aux alertes météorologiques », a déclaré David Harding. « S'il y a ne serait-ce que 10 % de risque de tornade, vous n'attendez pas. Vous vous mettez à l'abri. » Il a ajouté que ce niveau de risque n'est pas quelque chose que les responsables de la sécurité des systèmes d'information peuvent gérer seuls. « Le quantique est désormais une question qui se pose au niveau des conseils d'administration, et non plus seulement au niveau de l'ingénierie. L'ampleur de son impact fait passer le bug de l'an 2000 pour un simple échauffement. » Alors que les entreprises redoublent d'efforts pour améliorer les performances de l'IA, beaucoup restent dangereusement naïves quant aux risques inhérents à cette technologie. Comme l'a déclaré David Harding, « la question n'est plus de savoir si le quantique aura un impact sur les systèmes d'IA, mais à quelle vitesse les entreprises pourront s'adapter avant que cela ne se produise ». La sécurité de l'IA ne dépend pas seulement du cryptage, mais aussi de la capacité à anticiper la fragilité de l'ensemble de l'écosystème en cas de défaillance de ce cryptage. Si les pirates parviennent à décrypter, rediriger ou manipuler ces systèmes a posteriori, le coup porté à la confiance du public pourrait égaler, voire dépasser, celui causé par les cyberattaques précédentes. La confiance est ce qui donne son pouvoir à l'IA. Sans elle, même les modèles les plus intelligents s'effondreraient. « Nous avons bâti toute une ère de prise de décision sur des architectures qui pourraient s'avérer plus fragiles que nous le pensions », a déclaré David Harding. « Alors que les entreprises recherchent l'optimisation, leurs adversaires recherchent les clés. »Une contribution de Kolawole Samuel Adebayo pour Forbes US, traduite par Flora LucasÀ lire également : Préparer l'avenir numérique : enjeux et adoption de la cryptographie post-quantique en entreprise

Documents sauvegardés

L'AGEFI

Nom de la source
L'AGEFI Quotidien - Édition de 7h

Type de source
Presse • Journaux

Périodicité
Quotidien

Couverture géographique
Nationale

Provenance
France

Lundi 20 octobre 2025

L'AGEFI Quotidien - Édition de 7h

• p. 62,63

• 892 mots

Le quantique ouvre l'horizon des possibles des banques, en bien comme en mal

Séverine Charon

Les possibilités, en matière de valorisation et de modélisation des risques, suscitent des appétits chez nombre de banquiers. Ils imaginent des cas d'usage, notamment pour les activités de marché. La possible survenance du Q-Day, l'avènement de l'ordinateur quantique, constitue surtout une menace inédite sur la sécurité des échanges et des transactions.

Fin septembre, HSBC a indiqué avoir testé avec IBM l'informatique quantique pour optimiser ses performances sur le marché des obligations, avec des résultats qui montrent « *une amélioration de 34% dans la précision des prédictions de prix*». Enthousiaste, HSBC n'a pas hésité à évoquer un « *moment spoutnik* » Une dizaine de jours plus tard, le Crédit Agricole et Quandela se félicitaient de la mise au point d'une solution quantique qui permet de mieux prédire les risques de défaut de crédit. Ces deux annonces illustrent bien la compréhension par les banques des opportunités offertes par le calcul quantique dans le monde financier.

« *Le principe de l'ordinateur quantique est de reprendre ce que fait la nature pour le répliquer de manière contrôlée : ce mécanisme permet de résoudre des problèmes d'optimisation et des équations très complexes. Cela ouvre des perspectives sur de multiples cas d'usages positifs, comme le pricing d'options et l'évaluation des risques. Un certain nombre d'institutions financières se sont emparées du sujet, avec la mise en place de programmes de recherches et de publications. Elles se mobilisent pour être les premières à bénéficier de ces cas d'usages*», explique Jean-François Bobier, associé au sein du BCG, spécialiste des questions tech.

Le quantique pour avoir un coup d'avance

Les banques américaines, JPMorgan en tête, investissent dans le quantique, mais les européens ne veulent pas être en reste, comme en témoigne l'annonce de Crédit Agricole. Le groupe BPCE s'est aussi mis au quantique, pour imaginer des cas d'usage, et acculturer au quantique, qui constitue un champ de connaissances nouvelles et difficiles à appréhender, même quand on est informaticien. « *Le collectif a été lancé en mars 2024. Il rassemble l'ensemble des métiers du groupe en co-animation avec les équipes Innovation de BPCE. L'objectif vise déjà à identifier des cas d'usage. Dans le cadre du collectif, nous rencontrons les acteurs français et internationaux - les entreprises françaises sont parmi les meilleures sur le sujet. Et nous participons au Lab Quantique à la Station F*», détaille Laurent Fernandez, directeur du centre d'expertise technologique de BPCE.

Un ordinateur quantique pourrait casser environ 50% de la cryptographie actuelle utilisée par la quasi-totalité des solutions de sécurité
.

A lire aussi: Le quantique et l'identité numérique entrent dans la sécurité des moyens de paiement

« *Le collectif se réunit au minimum tous les trimestres, et nous intervenons régulièrement en interne pour partager ce qu'est le calcul quantique ou encore la cryptographie post-quantique dans des événements internes*» ajoute Pierre Léger, responsable Lab Innovation & Développement de BPCE.

La sensibilisation et la formation des ar-

Documents sauvegardés

mées d'informaticiens des banques est en effet un grand chantier. Si la mise au point de l'ordinateur quantique promet des possibilités de modélisations offrant des perspectives de business, elle ouvre aussi de manière certaine une brèche dans la sécurité. « *L'autre usage de l'ordinateur quantique, c'est l'algorithme de Shor. Celui-ci n'a qu'un usage, malfaisant, qui permet de décrypter la cryptographie publique utilisée pour sécuriser notamment les mails et les transactions*», résume Jean-François Bobier.

L'omniprésent chiffrage RSA menacé

« *Cela fait 40 ans qu'on utilise le chiffrage RSA, qui paraissait incassable. Il est présent partout, et notamment dans les fondations des architectures informatiques, sans qu'on ait pris la peine d'inventorier là où il était utilisé. Or le cryptage RSA ne résistera pas à l'ordinateur quantique. Pour l'instant, la taille des clés a été augmentée pour allonger le temps nécessaire pour casser le chiffrage, mais face à l'ordinateur quantique, cette riposte ne suffira pas*», prévient Jean-François Bobier. Le Crédit Mutuel, qui a annoncé il y a deux ans la prolongation dans le quantique d'un partenariat engagé dans l'IA avec IBM, cite comme domaine d'exploration la cybersécurité, la lutte contre la fraude en même temps que la modélisation des risques.

La grande difficulté réside dans le fait que la mise au point de l'ordinateur quantique doté de capacités de calcul suffisantes reste un événement dont la date de survenance est impossible à prédire. Dans cinq ans, c'est possible pour les plus optimistes, dans dix ans c'est fort possible, plus tard, c'est probable... « *On ne sait pas dire avec précision quand l'ordinateur quantique et le _Q-day' arriveront. Mais les banques doivent être prêtes avant. Le jour J, il sera trop tard*», prévient Jean-François Bobier. D'ailleurs, les autorités ne s'y trompent pas. La Banque de France vient d'annoncer qu'elle était parvenue à protéger les échanges de données des attaques d'un ordinateur quantique, et dès 2022, l'Agence nationale de la sécurité des systèmes d'information (Anssi) avertit de la nécessité de migrer vers la cryptographie post-quantique. Depuis, cette recommandation est devenue une obligation. « *La menace quantique, c'est la possibilité qu'un ordinateur quantique arrive sur le marché et casse environ cinquante pour cent de la cryptographie actuelle qui est utilisée par la quasi-totalité des solutions de sécurité fondées sur la cryptographie* », prédisait Raphaël Kenigsberg, coordinateur sectoriel finance à l'Anssi au cours d'une table ronde organisée lors de la dernière édition du Forum Fintech à la Banque de France. Personne ne sait dire quand surviendra le Q-Day, mais il faudra être prêt.

Documents sauvegardés

Nom de la source
L'AGEFI.fr
Type de source
Presse • Presse Web
Périodicité
En continu
Couverture géographique
Nationale
Provenance
France

Vendredi 17 octobre 2025

L'AGEFI.fr • 504 mots

Dans la sécurisation des paiements, le quantique entre en pratique

Alexandra Oubrier

Advanthink et Quandela travaillent ensemble depuis quelques mois sur un cas d'usage crucial, la détection de fraude, en complément des outils à base d'intelligence artificielle. Les premiers résultats sont encourageants.

Annoncée en juin dernier, la collaboration entre Advanthink et Quandela donne quelques résultats très intéressants. Mais ce n'est encore qu'un début. Advanthink (anciennement Isoft) a développé une plateforme qui sécurise les paiements et autres actions des clients des banques. Elle utilise largement l'intelligence artificielle et obtient de bons résultats. D'ailleurs, Advanthink est utilisé dans de nombreuses banques françaises et européennes, et au-delà.

Expérimenter

Mais la lutte contre la fraude aux paiements reste un jeu de gendarmes et de voleurs : l'avance de l'un ne dure jamais bien longtemps, l'autre le rattrape toujours. Et matière de fraude, mieux vaut avoir un coup d'avance pour préserver la sécurité des échanges. C'est pourquoi Brice Perdrix, son dirigeant, s'est intéressé à l'informatique quantique et a noué un partenariat avec Quandela. Cette start-up française a été fondée en 2017 avec pour objectif de construire un ordinateur quantique et des applications permettant de déployer la puissance de l'informatique quantique dans différents métiers.

A lire aussi: Advanthink choisit Quandela pour injecter du quantique dans la détection de fraudes

« *Dès son annonce, cette collaboration a suscité beaucoup de curiosité, nous avons reçu des demandes de personnes qui souhaitaient avoir accès à nos travaux* », indique Brice Perdrix. Une curiosité légitime : « *les algorithmes quantiques ont des spécificités qui permettent de détecter des patterns (schémas de fraude) que l'IA ne voit pas* », souligne Arno Ricou, chef d'équipe au sein de Quandela.

Un autre angle

Ainsi, avec les mêmes données que celles recueillies et traitées par l'IA, le quantique voit des fraudes qui n'ont pas été détectées. Ce n'est pas une question de quantité de données, l'apport du quantique ne réside pas tant dans le traitement de données massives, pour lequel le quantique peut se montrer moins performant, que dans sa capacité à regarder ces données sous un autre angle, ce qui permet de saisir des signaux faibles beaucoup plus fins. « *Le quantique étudie moins de données mais sous davantage d'axes*, explique Brice Perdrix, *c'est ce qui permet de mieux caractériser la différence entre un comportement normal ou anormal.* »

Ordinateur quantique construit par Quandela
. *©cyril marcilhacy / item*

A lire aussi: Quandela lève 50 millions d'euros auprès de plusieurs fonds

En pratique, Quandela propose des algorithmes quantiques qui sont intégrés dans la plateforme de data science, Amadea, d'Advanthink. Celle-ci simule le comportement d'une machine quantique, avec une puissance moindre, ce qui permet de tester des cas d'usage et de mesurer les résultats. « *C'est invisible pour les utilisateurs,* expose Arno Ricou, *mais cela permet de tester si une*

Documents sauvegardés

approche fonctionne sur l'informatique classique, en attendant 2027 et la disponibilité de notre ordinateur quantique. C'est alors que l'on pourra mesurer l'importance du changement dû au quantique. Nous sommes seulement aux prémices d'une nouvelle génération d'outils qui vont profondément transformer nos pratiques. »

A lire aussi: Quandela entre dans la course à l'ordinateur quantique photonique

Cet article est paru dans L'AGEFI.fr

https://www.agefi.fr/news/tech-finance/dans-la-securisation-des-paiements-le-quantique-entre-en-pratique?utm_source=cision&at_source=rss

Documents sauvegardés

news·20251022·CCMD·1000077_10254222919_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

Mercredi 22 octobre 2025

Le Journal du Net (JDN) (site web) - Le Journal du Net • 1197 mots

Développer une résilience post-quantique dans la sécurité des entreprises

Chronique de Krishna Narayanaswamy

Alors que l'informatique quantique poursuit sa progression de la théorie à la pratique, l'une des plus grandes menaces pour la sécurité des entreprises n'est désormais plus une perspective lointaine.

Selon une étude publiée par l'ANSSI, 50 % des organisations interrogées sont exposées à des risques liés aux futures attaques quantiques. Si les techniques de chiffrement classique ont jusqu'à présent bien protégé les utilisateurs et les entreprises, il devient donc urgent de développer des algorithmes et des implémentations chiffrées capables de résister à une attaque quantique. Dans cette quête, la Commission européenne a publié fin juin une feuille de route détaillée afin d'accompagner les Etats membres dans la transition vers des algorithmes de chiffrement résistants.

Au cœur des systèmes de chiffrement actuels, se trouvent des problèmes mathématiques que les ordinateurs classiques ont du mal à résoudre dans des délais raisonnables. Ils se divisent en deux catégories : les algorithmes de chiffrement symétrique comme l'Advanced Encryption Standard (AES) 256, et les algorithmes asymétriques comme Rivest-Shamir-Adleman (RSA), Diffie-Hellman et le chiffrement sur courbe elliptique (ECC).

Le développement de la sécurité post-quantique

Si les algorithmes symétriques semblent susceptibles de conserver leur efficacité après l'avènement de l'informatique quantique, un ordinateur quantique suffisamment puissant pourrait résoudre les algorithmes asymétriques en quelques heures, et non en plusieurs décennies, rendant ainsi obsolètes de nombreux systèmes de chiffrement actuels.

Bien qu'une utilisation généralisée des ordinateurs quantiques ne soit pas prévue avant plusieurs années, la menace qui pèse sur les données est bien réelle aujourd'hui. En effet, chaque fois que des cybercriminels exfiltrent des données chiffrées, ils collectent des actifs dans l'intention de les déchiffrer une fois que les capacités quantiques auront atteint leur maturité, une tactique connue sous le nom de collecter maintenant, déchiffrer plus tard (HNDL).

Ainsi, les RSSI doivent de toute urgence chercher à remplacer le chiffrement traditionnel vulnérable au sein de leur infrastructure numérique actuelle et entamer une transition vers le chiffrement post-quantique. Les instructions des régulateurs et des agences de cybersécurité sont claires sur ce passage à un chiffrement résistant aux attaques quantiques qui doit commencer dès maintenant.

L'identification des couches de chiffrement critiques

Tous les directeurs techniques, directeurs informatiques et RSSI se doivent d'évaluer collectivement leur infrastructure numérique afin de comprendre les endroits et les processus qui pourraient utiliser des chiffrements vulnérables. En envisageant le passage au chiffrement post-quantique, il convient de se concentrer dans un premier temps sur les données qui résident ou transitent en dehors de l'organisation. Pour les données qui résident et circulent au sein d'un réseau fiable, d'autres couches de sécurité plus traditionnelles, telles que le contrôle d'accès, seront essentielles pour faire face à la menace collecter maintenant, déchiffrer plus tard.

Documents sauvegardés

Des couches de chiffrement critiques, telles que le démarrage sécurisé, les échanges d'authentification et le chiffrement TLS, sont présentes dans la plupart des applications web et cloud et nécessitent une attention particulière. En s'appuyant sur ces exemples, il est possible d'identifier et de traiter les menaces similaires au sein de la pile technologique de toute organisation :

Chiffrement des données en transit entre services : dans une architecture cloud classique, de nombreux micro-services communiquent en permanence. Ces interactions sont chiffrées à l'aide de méthodes traditionnelles, mais devront être mises à niveau vers des algorithmes de chiffrement post-quantique afin de garantir la sécurité de ces canaux dans un monde post-quantique.

Chiffrement TLS pour l'inspection du trafic Web et des applications : en tant que fonction essentielle de toute pile de sécurité cloud, l'inspection du trafic Web et des applications chiffrés est cruciale pour appliquer les politiques et prévenir les menaces. Ce processus de déchiffrement et de rechiffrement TLS devra être amélioré à l'aide de mécanismes d'échange de clés post-quantiques dans un but de prévenir les risques d'interception.

Authentification client-cloud et échange de clés : lorsqu'un utilisateur se connecte à une plateforme cloud, des protocoles de chiffrement et d'authentification protègent ses données et son identité. Cette couche de connexion devra être réorganisée avec le chiffrement post-quantique afin de garantir l'intégrité de la génération de clés sécurisées et de l'authentification.

Protection des métadonnées internes : même lorsque les données sont chiffrées, les métadonnées telles que les informations de routage ou les journaux d'accès peuvent révéler des informations critiques. Ainsi, des protections post-quantiques au chiffrement des métadonnées internes doivent être appliquées afin d'éviter que ces informations ne deviennent un risque pour la sécurité de l'organisation.

Configuration client et chiffrement des données de politique : les fichiers de configuration spécifiques aux clients, les politiques de sécurité et les données stockées devront être protégés par un chiffrement quantique afin d'éviter toute exposition des données à long terme.

L'évolution de la conformité aux normes

Au cœur du déploiement du chiffrement post-quantique se trouve le respect des nouvelles normes du NIST. Publiées en août 2024, elles ont été élaborées en collaboration avec des universitaires, des agences gouvernementales et des entreprises technologiques de premier plan. Sur les quatre nouveaux algorithmes présentés, trois sont destinés aux signatures numériques et un à l'encapsulation de clés (CRYSTALS-Kyber, rebaptisé ML-KEM). ML-KEM 768, en particulier, s'avérera essentiel pour l'échange de clés dans le protocole d'établissement de connexion TLS en raison de ses performances, de son profil de sécurité et de son interopérabilité.

Les RSSI doivent s'assurer qu'ils comprennent bien les nouvelles échéances réglementaires, ainsi que les détails relatifs à la répartition des responsabilités. Par ailleurs, les organisations doivent s'appuyer sur leurs fournisseurs et s'assurer qu'ils communiquent leurs plans, avec des calendriers, tout en obtenant des informations utiles sur les autres éléments de la pile de sécurité qui pourraient nécessiter des changements, qu'ils soient menés par d'autres fournisseurs ou par l'organisation elle-même.

La mise en œuvre du chiffrement post-quantique et tests

Les nouveaux algorithmes de chiffrement post-quantique ne sont pas interchangeables. Ils ont des exigences de performance distinctes, ce qui a un impact différent sur les ressources en énergie et en mémoire. Les entreprises devront donc effectuer des tests approfondis dans un environnement sandbox afin d'éviter toute perturbation de leurs activités. Par exemple, l'intégration de matériel compatible avec le chiffrement post-quantique dans une pile de centres de données entraînera de nouvelles exigences en matière de puissance et de performance. Cela nécessitera un ajustement des ressources pour atteindre le niveau requis afin de prendre en charge les nouveaux outils d'IA.

Les fournisseurs d'applications et de services devraient procéder de la même manière, en proposant un déploiement contrôlé qui offre toutes les fonctionnalités grâce au chiffrement basé sur le post-quantique, permettant ainsi aux RSSI et aux équipes de sécurité de valider la compatibilité, les performances et l'efficacité dans des scénarios réels.

Un avantage stratégique indéniable

Dans un contexte où les menaces de cybersécurité évoluent rapidement et où les perturbations technologiques sont imminentes, la préparation quantique constituera un avantage concurrentiel à court terme et un impératif stratégique

Documents sauvegardés

à long terme. Cela est particulièrement évident lorsque les entreprises investissent massivement dans la mise en place d'une infrastructure de données pour soutenir l'adoption des technologies d'IA.

Toute initiative visant à intégrer le chiffrement post-quantique témoigne non seulement d'une sophistication technique, mais aussi d'une compréhension approfondie du changement de paradigme en matière de sécurité et de la menace qui pèse sur une ressource mondiale essentielle : les données.

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

https://www.journaldunet.com/cybersecurite/1545441-developper-une-resilience-post-quantique-dans-la-securite-des-entreprises/

Documents sauvegardés

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

Lundi 13 octobre 2025

Le Journal du Net (JDN) (site web) - Le Journal du Net • 730 mots

Sécurité quantique : menace existentielle ou avantage compétitif ?

Chronique de Michael Bittan

Les entreprises doivent dès maintenant se préparer à la transition vers la cryptographie post-quantique.

Promesse d'innovations majeures, l'informatique quantique est aussi une bombe à retardement pour la cybersécurité. Après la panne mondiale de juillet, les entreprises n'ont plus le luxe d'attendre : il est temps d'anticiper la transition vers la sécurité post-quantique.

La panne technologique mondiale de juillet 2025 restera longtemps dans les mémoires. Transports à l'arrêt, hôpitaux ralentis, communications perturbées : cet épisode a rappelé à quel point nos sociétés sont devenues dépendantes d'infrastructures numériques interconnectées, mais aussi vulnérables. Quelques jours ont suffi à faire vaciller des secteurs critiques. Pourtant, cette crise pourrait n'être qu'un avant-goût de bouleversements plus profonds encore, liés à l'essor de l'informatique quantique.

Car au-delà des bénéfices spectaculaires qu'elle promet (recherche médicale accélérée, optimisation logistique, intelligence artificielle de nouvelle génération) la puissance quantique représente aussi une menace directe pour la cybersécurité mondiale. Le chiffrement qui protège aujourd'hui nos échanges, nos transactions bancaires, nos données de santé ou encore nos identités numériques repose sur des verrous mathématiques considérés comme imprenables par les ordinateurs classiques. Demain, les machines quantiques pourraient les briser en quelques heures.

Quand l'avantage devient risque

Un ordinateur quantique n'est pas qu'un super ordinateur plus rapide. Grâce aux qubits, capables d'exister dans plusieurs états simultanément, il aborde certains problèmes réputés insolubles pour nos machines actuelles. La factorisation de grands nombres en est l'exemple le plus emblématique : c'est précisément ce problème qui fonde le chiffrement RSA, omniprésent dans nos communications numériques. Ce qui est aujourd'hui impraticable en temps humain pourrait devenir trivial pour une machine quantique mature.

Les premières victimes seraient probablement les secteurs les plus sensibles : banques, transports, communications, énergie. Mais aucune entreprise ne sera épargnée : de la start-up technologique aux géants industriels, tous dépendent de mécanismes cryptographiques vulnérables. Le scénario n'est plus de la science-fiction : des États investissent massivement pour atteindre cet avantage stratégique, et la criminalité organisée suivra rapidement.

La riposte post-quantique s'organise

Face à cette menace, la communauté scientifique et les organismes de normalisation travaillent depuis des années à développer de nouveaux standards de chiffrement résistants aux attaques quantiques. Le NIST (National Institute of Standards and Technology) s'apprête à publier les premières normes mondiales de cryptographie post-quantique. Une excellente nouvelle : la menace est inévitable, mais des solutions existent et commencent à se structurer.

Encore faut-il que les entreprises s'y préparent dès maintenant. Car la transition ne sera ni instantanée ni gratuite. Identifier tous les points de vulnérabilité, remplacer les algorithmes existants, déployer de nouvelles architectures de

Documents sauvegardés

sécurité, tester leur compatibilité : il s'agit d'un processus pluriannuel. Attendre le jour J où un chiffrement sera brisé par un acteur malveillant serait un pari à très haut risque.

Les trois priorités pour les entreprises

Évaluer le risque quantique : dresser un état des lieux des systèmes dépendants de la cryptographie actuelle et définir un plan de transition stratégique.

Cartographier les vulnérabilités : grâce à de nouveaux outils de découverte cryptographique, identifier où se cachent les algorithmes fragiles dans les applications, le cloud, les terminaux, chez ses partenaires.

Construire une architecture crypto-agile : intégrer les nouveaux standards post-quantiques du NIST, mais aussi préparer des mécanismes de gestion flexible, capables d'évoluer au rythme des menaces et des innovations, y compris la distribution de clés quantiques (QKD).

De la contrainte à l'opportunité

Aborder la sécurité quantique uniquement sous l'angle de la menace serait réducteur. Pour les entreprises, il s'agit aussi d'une occasion stratégique : renforcer leur résilience, restaurer la confiance numérique et se positionner en leaders d'un écosystème en mutation. Celles qui anticiperont la transition sécuriseront non seulement leurs actifs, mais gagneront aussi un avantage compétitif face à des concurrents moins préparés.

L'année 2025, proclamée par l'ONU Année du quantique , restera peut-être comme celle où les promesses technologiques se sont doublées d'une prise de conscience sécuritaire. Après la panne mondiale de juillet, les dirigeants ne peuvent plus ignorer que la prochaine grande crise numérique ne viendra pas forcément d'un bug ou d'une attaque classique, mais d'une rupture scientifique. Le temps est venu d'investir dans la préparation post-quantique. Car si la panne de juillet a été réparée en quelques jours, une faille cryptographique mondiale ne le sera pas.

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

https://www.journaldunet.com/cybersecurite/1545005-securite-quantique-menace-existentielle-ou-avantage-competitif/

Documents sauvegardés

Les Echos

Nom de la source
Les Echos
Type de source
Presse • Journaux
Périodicité
Quotidien
Couverture géographique
Nationale
Provenance
France

Jeudi 16 octobre 2025
Les Echos • no. 24568
• p. 29
• 540 mots
Banque centrale

La Banque de France se prépare au post-quantique

Les ordinateurs quantiques pourraient d'ici à une dizaine d'années « casser » les cryptographies et ainsi menacer le secteur bancaire.

« Il y aura un avant et un après-quantique et ce sera une réelle rupture technologique », avertit Raphaël Kenigsberg, coordinateur sectoriel finance à l'Anssi, lors de l'ouverture du forum Fintech de l'ACPR. D'ici à une dizaine d'années, les ordinateurs quantiques, en utilisant les propriétés de la matière à l'échelle de l'infiniment petit, seront assez puissants pour *« casser les cryptographies »* , soit les mécanismes de chiffrement qui protègent actuellement nos transactions et autres données sensibles.

« La menace de l'informatique quantique *est d'utiliser cette puissance de calcul pour pouvoir déchiffrer relativement facilement ce qui est chiffré aujourd'hui, et notamment des communications électroniques, en particulier dans le domaine financier »*, explique Valérie Fasquelle, directrice générale du système d'information à la Banque de France.

Si ces données se retrouvent entre les mains d'acteurs malveillants, ils pourraient alors contourner les systèmes d'authentification, usurper des identités numériques et accéder aisément à des bases de données sensibles, ouvrant potentiellement la voie à des fraudes massives.

Une première expérience de sécurisation

« Le secteur financier doit être conscient des risques et préparer sa transition », prévient Valérie Fasquelle. La semaine dernière, la banque centrale a annoncé le succès d'une expérimentation de sécurisation des données post-quantique.

Le test portait sur un échange de données de l'assureur Allianz à la Banque de France. *« L'idée était de garder exactement le même processus de communication, les mêmes briques techniques, les différentes applications ainsi que le système de gestion d'identité qui préexiste. Nous n'avons rien changé à la chaîne de liaison, nous avons simplement intégré des algorithmes de sécurisation post-quantique, aux différents endroits où il y avait une vérification des signatures »*, détaille la directrice.

Dans le cas de l'expérience, cela permet de vérifier qu'Allianz est bien celui qui communique ses données à la Banque, et que l'entreprise n'est pas victime d'une usurpation d'identité. Cette hybridation entre algorithmes de sécurisation déjà utilisés et ceux prévus pour résister à l'après-quantique, a permis *« une protection de bout en bout des données sensibles contre les menaces quantiques présentes et futures »*, se félicite l'institution bancaire dans son communiqué.

La technique « Store now, decrypt later »

En effet, même si les ordinateurs quantiques aujourd'hui en circulation ne sont pas encore assez puissants pour décrypter les informations cryptées, les menaces planent déjà. Une technique d'attaque, appelée « Store now, decrypt later », consiste pour les acteurs malveillants à capturer les informations sensibles et à les conserver en attendant l'arrivée des ordinateurs quantiques.

« Aujourd'hui, les données qui sont stockées ou transmises de manière sécurisée sont d'une certaine manière déjà exposées aux attaques post-quantiques. C'est pour ça que nous sommes très attentifs aux attaques cyber, *parce que derrière chaque attaque qui vise à dérober des données, se cache un potentiel décryptage post-quantique dans quelques années »*, anticipe Valérie Fasquelle. La banque centrale a dressé sa feuille de route pour s'adapter à cette

Documents sauvegardés

nouvelle ère, avec comme première étape la réalisation d' *« un inventaire de tous les dispositifs de sécurité et donc de signatures des systèmes d'information »*, précise Valérie Fasquelle. L'idée n'est ainsi pas d'utiliser des algorithmes post-quantiques sur l'ensemble de ses données, mais plutôt de hiérarchiser les données en fonction de leur sensibilité.

Juliette Roussel

Documents sauvegardés

Epargnons Responsable! (site web) - Epargnons Responsable!

Nom de la source
Epargnons Responsable! (site web) - Epargnons Responsable!

Type de source
Presse • Presse Web

Périodicité
En continu

Couverture géographique
Nationale

Provenance
Audun-le-Roman, Grand Est, France

Friday, October 17, 2025

Epargnons Responsable! (site web) - Epargnons Responsable! • 365 mots

LexisNexis

[Question de Gestion] L’innovation quantique au service de la finance

Crédit Agricole CIB et Quandela optimisent les modèles de prédiction des risques de défaut

Crédit Agricole CIB et Quandela, acteur européen de premier plan dans le domaine de l'informatique quantique, dévoilent aujourd'hui les résultats significatifs de leur collaboration visant à développer une solution quantique dédiée à la prédiction des risques de défaut de crédit.

Dans le cadre de cette collaboration, les équipes de Crédit Agricole CIB et Quandela ont conjointement élaboré un algorithme classique-quantique novateur qui démontre une amélioration de la performance prédictive du modèle de risque par rapport aux méthodes de calcul classiques. Cette avancée, pour la première fois validée sur des processeurs quantiques photoniques, confirme son applicabilité dans un environnement financier.

L’amélioration obtenue ouvre des perspectives prometteuses pour l'industrie financière dans la gestion de ses risques ou l’optimisation de portefeuille. Plus largement ces résultats montrent l’intérêt des collaborations entre acteurs du quantique et acteurs financiers.

Pierre Dulon, Directeur général adjoint de Crédit Agricole CIB en charge de IT & Operations Services, explique : « La complémentarité des algorithmes classiques et algorithmes quantiques ouvre de nouvelles voies dans notre stratégie pour le calcul intensif, notamment dans les domaines de la prévention des risques ou dans l’optimisation des ressources rares. Cette nouvelle collaboration avec un acteur majeur du secteur confirme l’engagement de Crédit Agricole CIB dans les technologies quantiques »

Niccolo Somaschi, co-fondateur et CEO de Quandela, conclut :« Cette collaboration avec Crédit Agricole CIB démontre que l'informatique quantique est désormais prête à relever des défis concrets dans le secteur financier. L'amélioration concrète que nous avons obtenue sur nos ordinateurs quantiques pour la prédiction des défauts n'est qu’un début. Notre feuille de route technologique et l'expertise de nos équipes nous permettront d'amplifier ces gains de performance dans les prochains mois, offrant ainsi un avantage compétitif significatif à nos partenaires qui adoptent ces solutions hybrides quantiques-classiques. »