BLOG

L'INFORMATIQUE QUANTIQUE expliquée simplement

31 juillet 2026 - Denis Favre

> *De la puce Willow au Q-Day : ce qui change vraiment, et pourquoi cela vous concerne déjà*

Temps de lecture estimé : 25 minutes

Cinq minutes contre dix millions de milliards de milliards d'années

Le 9 décembre 2024, Google publie dans la revue Nature un article au titre volontairement technique : « Correction d'erreurs quantiques sous le seuil du code de surface ». Le grand public retient surtout un chiffre spectaculaire. La nouvelle puce du laboratoire, baptisée Willow, vient de boucler en moins de cinq minutes un calcul de référence que les supercalculateurs les plus puissants de la planète mettraient environ 10 septillions d'années à reproduire.

Précisons tout de suite ce nombre, parce qu'il circule mal. Dans la convention anglo-saxonne utilisée par Google, « 10 septillion » signifie 10 puissance 25 années, soit 1 suivi de 26 zéros. L'univers, lui, a environ 13,8 milliards d'années. Le calcul de Willow dépasse donc l'âge de l'univers d'un facteur d'environ mille milliards de milliards. Ce n'est pas une avance technologique : c'est un changement de catégorie.

À partir de là, deux réactions coexistent, et elles sont toutes les deux justifiées. La première : quelque chose de réel vient de se produire, après trente ans d'impasse théorique. La seconde : ce calcul précis ne sert strictement à rien. Il ne soigne aucun cancer, n'optimise aucun portefeuille, ne casse aucun chiffrement. C'est un test de laboratoire, choisi précisément parce qu'il est difficile pour une machine classique.

Cet article a pour but de vous donner de quoi tenir les deux bouts : comprendre ce qu'un ordinateur quantique fait réellement, ce qu'il ne fera jamais, où en est la course industrielle en 2026, et surtout quelle est la seule échéance qui vous concerne dès aujourd'hui, même si vous ne toucherez jamais une de ces machines — la cryptographie.

1. Ce qu'est un ordinateur quantique (et ce qu'il n'est pas)

Le bit classique : une réponse à la fois

Un ordinateur classique — celui sur lequel vous lisez cette page — raisonne en bits. Un bit, c'est un état parmi deux possibles : 0 ou 1. Toute la puissance de l'informatique moderne repose sur l'empilement d'un nombre vertigineux de ces états binaires et sur la vitesse à laquelle on les manipule.

Cette architecture a une conséquence structurelle : pour explorer un espace de possibilités, la machine doit les tester les unes après les autres. Elle peut le faire très vite, et en parallèle sur plusieurs cœurs, mais elle reste fondamentalement séquentielle. Face à certains problèmes, le nombre de combinaisons croît si vite que même en multipliant les processeurs, on n'y arrive pas avant la fin des temps.

Le qubit et la superposition

Un qubit — pour quantum bit — n'est pas un composant électronique au sens habituel. C'est un objet physique microscopique : un circuit supraconducteur refroidi à l'extrême, un ion piégé par des lasers, un atome neutre maintenu par des pinces optiques, un photon. Ces objets obéissent aux lois de la mécanique quantique, et l'une d'elles s'appelle la superposition.

La superposition autorise le qubit à ne pas trancher entre 0 et 1 tant qu'on ne le mesure pas. Il occupe une combinaison des deux états, décrite par des nombres appelés amplitudes de probabilité.

> *L'image de la bibliothèque : un ordinateur classique cherche un livre en parcourant les rayons un par un. Un ordinateur quantique explore l'ensemble des rayons simultanément. L'image est utile pour comprendre l'idée — mais elle est trompeuse si on s'arrête là, car au moment de la mesure, la machine ne rend qu'une seule réponse. Tout l'art consiste à s'arranger pour que ce soit la bonne.*

L'intrication : le second ingrédient

La superposition seule ne suffit pas. Ce qui donne aux ordinateurs quantiques leur puissance, c'est l'intrication. Lorsque deux qubits sont intriqués, leurs états ne peuvent plus être décrits séparément : mesurer l'un détermine instantanément ce que l'on trouvera sur l'autre, quelle que soit la distance qui les sépare.

Einstein trouvait ce phénomène si contre-intuitif qu'il le qualifiait d'action fantôme à distance et y voyait la preuve que la théorie quantique était incomplète. L'expérience lui a donné tort : l'intrication a été vérifiée en laboratoire de façon répétée, et les travaux qui l'ont établie ont valu le prix Nobel de physique 2022 à Alain Aspect, John Clauser et Anton Zeilinger.

Concrètement, l'intrication permet à un registre de qubits de représenter un espace d'états exponentiellement plus grand que le nombre de qubits. Avec 300 qubits parfaitement intriqués, on décrit davantage d'états qu'il n'y a d'atomes dans l'univers observable.

L'interférence : le véritable moteur

C'est le mécanisme le moins souvent expliqué, et pourtant le plus important. Puisque la mesure ne rend qu'une seule réponse, il faut faire en sorte que les mauvaises réponses s'annulent entre elles et que la bonne ressorte. C'est exactement ce que fait l'interférence quantique, sur le modèle des ondes qui s'amplifient quand elles sont en phase et s'annulent quand elles sont en opposition.

Un algorithme quantique n'est donc pas une recherche parallèle : c'est une chorégraphie d'interférences. On prépare une superposition, on la fait évoluer de façon à ce que les amplitudes des mauvais résultats se détruisent mutuellement, et on mesure. Cette contrainte explique pourquoi il n'existe pas des milliers d'algorithmes quantiques utiles : concevoir cette chorégraphie est extraordinairement difficile, et elle ne fonctionne que pour des familles de problèmes bien particulières.

	Ordinateur classique	Ordinateur quantique
Unité de base	Le bit : 0 ou 1	Le qubit : superposition de 0 et 1
Mode d'exploration	Séquentiel, une combinaison à la fois	Amplitudes manipulées globalement, résultat extrait par interférence
Fiabilité d'une opération	Erreur quasi nulle (10⁻¹⁵ et moins)	De l'ordre de 1 erreur sur 100 à 1 sur 1 000 opérations physiques
Environnement	Ambiant, ventilateur suffisant	Quelques millikelvins, cryostat et blindage
Champ d'application	Universel : bureautique, web, vidéo, IA	Très étroit : simulation quantique, optimisation, factorisation

	Disponibilité	Cloud, quelques dizaines de machines dans le monde

Ce qu'un ordinateur quantique ne fera jamais

C'est le point que la plupart des articles grand public escamotent. Un ordinateur quantique ne remplacera pas votre machine. Il ne lira pas vos e-mails plus vite, ne fera pas tourner Netflix, ne compilera pas votre code. Pour l'immense majorité des tâches, il est infiniment moins efficace qu'un processeur classique à quinze euros.

Son rôle est celui d'un accélérateur spécialisé, comparable à ce qu'est un GPU pour le calcul matriciel : une machine que l'on interroge sur une sous-partie très précise d'un problème, dans un pipeline dont le reste demeure classique. Toutes les architectures crédibles annoncées pour la fin de la décennie sont d'ailleurs hybrides : un supercalculateur classique pilote une unité de traitement quantique, la QPU.

2. Pourquoi vous n'en avez pas un sur votre bureau

La décohérence, ennemie numéro un

Les qubits sont d'une fragilité difficile à imaginer. Une vibration, un champ électromagnétique parasite, un photon égaré, une variation infime de température : l'état quantique se dégrade et l'information est perdue. C'est ce qu'on appelle la décohérence.

On la mesure par des temps de cohérence. Sur la génération précédente de puces Google, la durée de vie moyenne d'un qubit était d'environ 20 microsecondes. Willow l'a portée à environ 68 microsecondes. On parle donc de quelques centièmes de milliseconde pour effectuer l'intégralité d'un calcul avant que l'information ne se dissolve.

Le froid extrême

Pour ralentir la décohérence, on refroidit. Les puces supraconductrices fonctionnent à quelques millièmes de degré au-dessus du zéro absolu, c'est-à-dire aux alentours de −273,14 °C. C'est plus froid que l'espace interstellaire, dont la température de fond avoisine −270 °C.

Ces fameuses photographies de lustres dorés suspendus que l'on associe aux ordinateurs quantiques ne montrent d'ailleurs pas la puce : ce sont les étages du réfrigérateur à dilution, chaque plateau correspondant à un palier de température de plus en plus bas. La puce elle-même, minuscule, se trouve tout en bas.

Toutes les technologies n'imposent pas ces conditions. Les ordinateurs photoniques — spécialité de la française Quandela — travaillent sur des photons et évitent une partie de ces contraintes cryogéniques. Les atomes neutres de Pasqal fonctionnent avec une consommation électrique bien plus faible que les architectures supraconductrices. Il n'existe pas une seule voie technologique, mais plusieurs paris concurrents, et personne ne sait encore lequel l'emportera.

La correction d'erreurs : le verrou historique

Voilà le cœur du problème, et c'est ici que se joue toute l'histoire de décembre 2024. Un qubit se trompe environ une fois sur mille opérations, parfois plus. Or les algorithmes utiles — factoriser une clé, simuler une molécule complexe — exigent des milliards, voire des milliers de milliards d'opérations enchaînées. Avec un tel taux d'erreur, le résultat est du bruit.

La parade théorique est connue depuis le milieu des années 1990, grâce notamment aux travaux de Peter Shor : on encode l'information d'un qubit utile, dit qubit logique, dans un ensemble de qubits physiques disposés en grille. La redondance permet de détecter et de corriger les erreurs en temps réel, sans jamais lire directement l'information protégée.

Mais cette théorie n'avait de sens que si l'on descendait sous un seuil critique de fidélité. Au-dessus de ce seuil, ajouter des qubits pour corriger introduit plus d'erreurs que cela n'en supprime : le système se dégrade au lieu de s'améliorer. Pendant près de trente ans, aucune machine n'était passée sous ce seuil. C'était le mur.

Notion	Ce que c'est
Qubit physique	Le composant réel gravé sur la puce. Bruité, fragile, éphémère.
Qubit logique	Un qubit fiable, reconstitué à partir de dizaines ou de milliers de qubits physiques via un code correcteur.
Code de surface	Le code correcteur le plus utilisé : une grille 2D de qubits physiques. Robuste, mais très gourmand.

Distance du code	La taille de la grille (3, 5, 7…). Plus elle est grande, plus la protection est forte, plus il faut de qubits.
Sous le seuil	Le régime où augmenter la distance du code fait baisser le taux d'erreur au lieu de l'augmenter.

3. Willow, décembre 2024 : ce qui a réellement changé

Le franchissement du seuil

Willow est une puce supraconductrice de 105 qubits physiques. L'équipe de Google Quantum AI y a implanté des mémoires en code de surface de distance 3, 5 puis 7, et a mesuré le taux d'erreur logique à chaque étape.

Le résultat est celui que trente ans de recherche attendaient : chaque fois que la distance du code augmentait de deux, le taux d'erreur logique était divisé par un facteur d'environ 2,14. Autrement dit, plus on ajoute de qubits, moins le système se trompe. La courbe s'est inversée. Le code de distance 7, mobilisant 101 qubits, affichait un taux d'erreur d'environ 0,14 % par cycle de correction.

Deuxième résultat, aussi important et moins commenté : ce qubit logique vivait plus longtemps que le meilleur des qubits physiques qui le composaient, d'un facteur d'environ 2,4. La correction d'erreurs ne se contentait plus de compenser son propre coût : elle produisait un gain net. Et le décodage — le calcul classique qui identifie les erreurs à corriger — fonctionnait en temps réel, avec une latence de quelques dizaines de microsecondes, ce qui était l'autre difficulté d'ingénierie.

Le benchmark des cinq minutes, et ce qu'il vaut

Le calcul spectaculaire cité en introduction relève d'un exercice précis appelé Random Circuit Sampling, ou échantillonnage de circuits aléatoires. On demande à la machine de produire des tirages issus d'un circuit quantique aléatoire, tâche choisie parce qu'elle est très difficile à simuler classiquement.

Ce test n'a aucune application pratique. Il ne conçoit rien, ne prédit rien, ne résout aucun problème posé par un être humain. Sa seule vertu est de démontrer que l'architecture matérielle fonctionne à l'échelle annoncée. Confondre ce benchmark avec une percée applicative est la première erreur d'interprétation à éviter.

Pourquoi 2024 n'est pas 2019

En 2019, Google avait déjà annoncé la « suprématie quantique » avec sa puce Sycamore. IBM avait contesté publiquement le résultat en quelques jours, en montrant qu'une simulation classique mieux optimisée réduisait considérablement l'écart annoncé. L'épisode avait laissé un goût amer et alimenté durablement le soupçon.

Le résultat de 2024 est d'une autre nature. Il ne repose pas sur une comparaison de vitesse contestable, mais sur une mesure physique interne au dispositif : le taux d'erreur logique décroît quand la taille du code augmente. C'est vérifiable, reproductible, et aucune contre-argumentation sérieuse n'a été publiée depuis. Le silence des concurrents, ici, vaut validation.

4. 2025-2026 : la course s'accélère

Google : l'avantage quantique « vérifiable »

En octobre 2025, Google publie un second résultat dans Nature, autour d'un algorithme baptisé Quantum Echoes. L'annonce revendique un avantage quantique vérifiable : le calcul aurait tourné environ 13 000 fois plus vite que le meilleur algorithme classique connu sur le plus puissant supercalculateur disponible, et surtout son résultat serait reproductible sur une autre machine quantique de qualité comparable.

La nuance est importante. Les tirages du Random Circuit Sampling n'étaient pas vérifiables autrement qu'en refaisant le calcul classique. Ici, la grandeur mesurée est une valeur moyenne physique, du type de celles qu'un autre laboratoire peut confirmer. Google évoque des applications en résonance magnétique nucléaire et en détermination de structures moléculaires.

Une partie de la communauté scientifique est restée sceptique, et Nature elle-même a relayé ces réserves. Les critiques portent sur deux points : la tâche reste taillée pour la machine plutôt que dictée par un besoin réel, et la vérification croisée sur un second processeur n'avait pas été effectuée au moment de la publication. Le progrès est réel ; le mot « application » reste prématuré.

IBM : une feuille de route datée

IBM a choisi une stratégie différente et beaucoup plus explicite. En novembre 2025, l'entreprise dévoile Nighthawk, un processeur de 120 qubits relié par 218 coupleurs accordables de nouvelle génération, permettant des circuits environ 30 % plus complexes que la génération Heron. Objectif affiché : un avantage quantique vérifié par la communauté scientifique d'ici fin 2026.

En parallèle, IBM a présenté Loon, un processeur expérimental destiné à valider sur une seule puce tous les composants matériels nécessaires à la tolérance aux fautes, et publie un calendrier inhabituellement précis : Kookaburra en 2026 pour la mémoire quantique en codes qLDPC, puis Starling en 2029, visant 200 qubits logiques construits à partir d'environ 10 000 qubits physiques. IBM revendique que ses codes qLDPC demandent environ 90 % de qubits en moins que le code de surface employé par Google.

Cette course de calendrier a un mérite : elle est falsifiable. Fin 2026, on saura si l'avantage quantique annoncé a été validé ou non.

L'argent, et ce qu'il raconte

Le baromètre de référence du secteur, le Quantum Technology Monitor publié chaque année par McKinsey, a revu ses projections nettement à la hausse dans son édition 2026. La valeur économique cumulée que l'informatique quantique pourrait créer d'ici 2035 y est estimée entre 1 300 et 2 700 milliards de dollars, contre 1 300 milliards dans les éditions précédentes.

Les chiffres de court terme sont plus parlants que ces projections : le secteur a franchi pour la première fois le milliard de dollars de chiffre d'affaires réel en 2025, avec une projection à 4,4 milliards pour 2028. Plus de 300 entreprises dans le monde travaillent désormais avec des fournisseurs de technologies quantiques, parmi lesquelles Airbus, JPMorgan Chase ou Boehringer Ingelheim. Un tiers des organisations analysées y consacrent plus de 10 millions de dollars par an.

Deux signaux méritent d'être relevés. D'abord la bascule vers le privé : en 2025, le financement privé représentait environ 97 % des montants investis, contre 67 % l'année précédente. Ensuite la concentration : environ 60 % des investissements de 2025 se sont portés sur les dix plus grosses opérations. Le secteur sort de la recherche publique et entre dans une logique industrielle — avec les effets de bulle qui accompagnent généralement ce type de transition.

Où en est la France ?

La France n'est pas spectatrice, contrairement à ce que l'on entend souvent. Le plan quantique national lancé en janvier 2021 a mobilisé 1,8 milliard d'euros d'investissements publics sur 2021-2025 via France 2030. Il a été complété en mars 2024 par PROQCIMA, un programme de 500 millions d'euros piloté par la Direction générale de l'armement, et prolongé en mai 2026 par un engagement supplémentaire d'un milliard d'euros sur 2026-2030.

PROQCIMA présente une originalité qui n'a pas d'équivalent ailleurs : plutôt que de miser sur une seule technologie, l'État finance simultanément cinq architectures de qubits concurrentes, portées par cinq start-up, dans une course à élimination progressive — cinq candidats au départ, trois après quatre

ans, deux après huit ans.

Entreprise	Technologie de qubit	Repère
Pasqal	Atomes neutres piégés par pinces optiques	Machine Ruby (100 qubits) installée au TGCC du CEA ; projet de cotation au Nasdaq annoncé en 2026
Quandela	Photonique (photons uniques)	Machine Lucy livrée au CEA, présentée comme le plus puissant calculateur photonique d'Europe
Alice & Bob	Qubits de chat, orientés tolérance aux fautes	Machine Kity attendue au CEA à l'horizon 2027
Quobly	Spins sur silicium (compatible CMOS)	Pari sur la réutilisation des chaînes de fabrication de semi-conducteurs
C12	Nanotubes de carbone	Laboratoire souterrain à Paris pour minimiser les vibrations

Le retard européen est réel sur les montants privés — le patron de Bpifrance a publiquement alerté en 2025 sur la sous-participation du capital privé européen face aux États-Unis et à la Chine. Mais il est nettement moins marqué sur la recherche et sur la diversité technologique, où la France occupe une position singulière.

5. À quoi cela va servir concrètement

Passons aux cas d'usage. Ils sont réels, mais leur maturité varie énormément, et il est utile de les classer par ordre de crédibilité décroissante.

La chimie et les matériaux : le cas d'usage le plus naturel

C'est de loin l'application la plus solide, pour une raison de principe : simuler une molécule, c'est simuler un système quantique. Un ordinateur classique doit approximer ce comportement avec des méthodes coûteuses dont l'erreur croît avec la taille du système ; un ordinateur quantique le représente nativement.

Les retombées attendues : catalyseurs plus efficaces pour la production d'engrais ou d'hydrogène, nouvelles chimies de batteries, matériaux supraconducteurs. Ce sont aussi les domaines où les besoins en qubits logiques sont les plus modestes, donc ceux qui arriveront probablement en premier.

La pharmacie et la biologie

Même logique appliquée au vivant : comprendre comment une molécule candidate va se lier à une protéine cible suppose de modéliser un très grand nombre d'interactions quantiques. Les estimations les plus optimistes évoquent une réduction du délai de développement d'un médicament de dix à quinze ans aujourd'hui vers deux à trois ans.

Il faut recevoir ce chiffre avec prudence. Le goulot d'étranglement du développement pharmaceutique n'est pas seulement le calcul : ce sont les essais cliniques, la réglementation, le recrutement de patients. Le quantique peut accélérer la phase de découverte ; il ne raccourcira pas une phase III. McKinsey reconnaît d'ailleurs explicitement que l'impact attribué au quantique dans ce secteur se recoupe partiellement avec celui de l'IA générative.

La finance

Optimiser un portefeuille de mille actifs sous cinquante contraintes, calculer des valeurs à risque, pricer des dérivés complexes : ce sont des problèmes d'optimisation et d'échantillonnage sur lesquels des institutions comme HSBC ou JPMorgan Chase mènent des expérimentations depuis plusieurs années.

Nuance nécessaire : à ce stade, les gains démontrés sur des instances réalistes restent modestes et souvent contestés par des méthodes classiques améliorées en réaction. Le secteur financier investit surtout pour ne pas se réveiller en retard, ce qui est une motivation parfaitement rationnelle.

L'énergie et la logistique

Équilibrer un réseau électrique alimenté par des milliers de sources renouvelables intermittentes, router une flotte de dix mille véhicules de livraison, ordonnancer une chaîne de production : ce sont des problèmes d'optimisation combinatoire, terrain de jeu théorique des algorithmes quantiques.

C'est aussi le domaine où le scepticisme est le plus fondé. Les heuristiques classiques sont excellentes sur ces problèmes, et l'avantage quantique promis y est le plus difficile à démontrer proprement.

Et l'intelligence artificielle ?

C'est le rapprochement le plus fréquent dans les discours commerciaux, et le plus fragile. À ce jour, aucun résultat ne montre qu'un ordinateur quantique accélérerait significativement l'entraînement des grands modèles de langage. Les gains théoriques identifiés en apprentissage automatique quantique portent sur des cas particuliers et supposent souvent que les données soient déjà chargées dans un état quantique — problème non résolu qui annule fréquemment le bénéfice attendu.

Le lien réel entre quantique et IA passe pour l'instant par l'inverse : c'est l'IA classique qui aide à concevoir, calibrer et décoder les systèmes quantiques.

6. Le vrai sujet à court terme : la cryptographie

S'il ne fallait retenir qu'une chose de tout cet article, ce serait cette partie. C'est le seul volet où l'informatique quantique impose des décisions concrètes, datées, à des organisations qui n'achèteront jamais d'ordinateur quantique.

Sur quoi repose la sécurité d'Internet

La quasi-totalité des échanges numériques est protégée par de la cryptographie asymétrique — essentiellement RSA et les courbes elliptiques. Votre connexion HTTPS, votre accès bancaire, la signature des mises à jour logicielles, les VPN d'entreprise, les cartes à puce : tout repose sur la même hypothèse. Certains problèmes mathématiques, comme la factorisation de très grands nombres ou le logarithme discret, sont hors de portée d'un ordinateur classique.

Cette hypothèse est parfaitement solide face au calcul classique. Elle ne l'est pas face à un ordinateur quantique. L'algorithme de Shor, publié en 1994, résout ces deux problèmes en temps polynomial. Ce qui demanderait des milliards d'années à un supercalculateur deviendrait affaire d'heures pour une machine quantique suffisamment grande et suffisamment fiable.

Ce qui n'est pas menacé

Précision essentielle, et rarement faite : la cryptographie symétrique n'est pas cassée par le quantique. AES et les fonctions de hachage modernes subissent l'algorithme de Grover, qui divise environ par deux la longueur effective des clés. La contre-mesure est triviale : passer d'AES-128 à AES-256 et utiliser des empreintes plus longues. Ce n'est pas là que se situe le danger.

Le Q-Day et la moisson anticipée

Le Q-Day désigne le jour où un ordinateur quantique tolérant aux fautes atteindra une taille suffisante pour casser les chiffrements en usage. Les enquêtes annuelles menées auprès des experts du domaine convergent depuis plusieurs années vers une fenêtre 2030-2035, avec une estimation médiane que les planificateurs de sécurité situent plutôt autour de 2033-2035.

Mais l'échéance qui compte n'est pas celle-là. Elle est déjà passée. Le scénario dit « Harvest Now, Decrypt Later » — moissonner maintenant, déchiffrer plus tard — consiste, pour un acteur étatique, à collecter dès aujourd'hui des flux chiffrés qu'il ne sait pas lire, en pariant sur leur déchiffrement futur. Le stockage coûte quasiment rien ; l'attente ne coûte rien du tout.

> *La règle de décision est simple : additionnez la durée pendant laquelle vos données doivent rester confidentielles et le temps qu'il vous faudra pour migrer votre parc. Si le total dépasse la date estimée du Q-Day, vous êtes déjà en retard. Pour un dossier médical, un secret industriel, un contrat ou une donnée d'état civil, la durée de confidentialité se compte en décennies.*

La réponse : la cryptographie post-quantique

La parade ne consiste pas à acheter des ordinateurs quantiques, mais à changer d'algorithmes. La cryptographie post-quantique — PQC — regroupe des algorithmes qui tournent sur des machines classiques ordinaires, mais reposent sur des problèmes mathématiques que l'on croit résistants aux attaques quantiques, principalement issus de la théorie des réseaux euclidiens.

Le NIST américain a standardisé les premiers d'entre eux en août 2024, à l'issue d'un concours international ouvert en 2016 : ML-KEM (issu de CRYSTALS-Kyber) pour l'échange de clés, ML-DSA (issu de CRYSTALS-Dilithium) et SLH-DSA (issu de SPHINCS+) pour la signature, complétés par Falcon. Ces algorithmes sont désormais implémentés dans les principales bibliothèques et navigateurs.

Le calendrier réglementaire, en clair

Échéance	Ce qui se passe
Août 2024	Le NIST publie les premiers standards PQC. Point de départ officiel de la migration mondiale.

2026	Phase d'inventaire cryptographique et de gouvernance recommandée par le Campus Cyber et l'ANSSI.
2027	L'ANSSI n'accorde plus de visa de sécurité aux produits dépourvus de mécanismes post-quantiques.
2030	Le NIST déprécie RSA et les courbes elliptiques pour les nouveaux usages. L'ANSSI juge déraisonnable d'acheter après cette date un produit sans PQC. Les cas d'usage à risque élevé doivent avoir migré.
2033-2035	Fenêtre médiane estimée pour le Q-Day.
2035	Interdiction totale de RSA et des courbes elliptiques côté NIST ; objectif de transition complète côté ANSSI et Commission européenne.

Ces échéances ne sont pas de même nature. Le cadre NIST relève d'une normalisation volontaire, sans force contraignante en Europe. Le cadre ANSSI est opposable pour les produits visant une qualification, pour les systèmes d'information d'importance vitale et pour les données classifiées. Mais l'effet de cliquet est mécanique : dès lors que la France et les États-Unis exigent la PQC pour leurs marchés publics, aucun éditeur international ne maintiendra deux gammes de produits. La cryptographie résistante au quantique devient le standard par défaut.

Deux textes européens accélèrent encore le mouvement : le Cyber Resilience Act, entré en vigueur en décembre 2024, impose des obligations dès décembre 2027 à tout produit connecté commercialisé en Europe ; et DORA, effectif depuis janvier 2025, exige des entités financières un inventaire cryptographique exhaustif et une véritable crypto-agilité.

7. Séparer le hype de la réalité

Un vocabulaire piégé

Trois expressions circulent, souvent confondues, et cette confusion est la principale source de malentendus.

Terme	Ce qu'il signifie réellement
Suprématie quantique	La machine bat les ordinateurs classiques sur une tâche artificielle, choisie pour lui être favorable. Aucune utilité pratique. Atteint en 2019, consolidé en 2024.
Avantage quantique	La machine bat les ordinateurs classiques sur un problème ayant une valeur pour quelqu'un. Revendiqué par Google en 2025, visé par IBM pour fin 2026, encore débattu.
Utilité quantique	La machine résout un problème réel mieux, moins cher ou plus vite qu'une alternative classique déployée en production. Nulle part atteint à ce jour.

Nous sommes encore dans l'ère NISQ

Les chercheurs qualifient la période actuelle d'ère NISQ — Noisy Intermediate-Scale Quantum, machines bruitées de taille intermédiaire. Concrètement : quelques dizaines à quelques centaines de qubits physiques, des taux d'erreur qui interdisent les circuits profonds sans correction, et une poignée de qubits logiques au mieux.

Le passage à un ordinateur quantique tolérant aux fautes à grande échelle suppose des milliers de qubits logiques, donc probablement des centaines de milliers à des millions de qubits physiques. Les feuilles de route les plus agressives visent 2029 pour les premiers systèmes tolérants aux fautes. C'est demain à l'échelle d'une DSI ; c'est loin à l'échelle d'un cycle produit.

Les signaux d'alerte à repérer

Un chiffre de qubits brandi sans mention du taux d'erreur ni de la connectivité : le nombre de qubits physiques seul ne veut rien dire.

Une comparaison de vitesse avec « le meilleur supercalculateur » sans préciser quel algorithme classique a servi de référence : c'est exactement ce qui a fait tomber la revendication de 2019.

Une promesse de disruption de l'IA par le quantique : à ce jour, rien ne l'étaye.

Une annonce de rupture cryptographique imminente sur Bitcoin ou RSA : casser une clé RSA-2048 demanderait, selon les estimations les plus sérieuses, des millions de qubits physiques.

Un fournisseur qui vend une « solution quantique » sans être capable de nommer le problème classique qu'elle bat, et de combien.

Ce que le quantique partage — et ne partage pas — avec l'IA

La comparaison avec la vague de l'IA générative est tentante, et elle est trompeuse. L'IA s'est diffusée par le bas : chacun a pu tester ChatGPT en trois clics et se forger une opinion. L'informatique quantique restera invisible pour le grand public. Ce n'est pas une application sur un téléphone, c'est une couche d'infrastructure.

Un utilisateur ne saura jamais qu'une QPU a participé au calcul du catalyseur qui a permis de fabriquer sa batterie, ou à l'optimisation du réseau qui a acheminé son électricité. Cette invisibilité a une conséquence pratique : elle rend le sujet plus difficile à porter en interne, à budgéter, à arbitrer face à des projets dont la démonstration est immédiate.

8. Que faire, concrètement

Si vous êtes un particulier

Peu de choses, et c'est une bonne nouvelle. Vos navigateurs, vos messageries et vos systèmes d'exploitation intègrent progressivement les algorithmes post-quantiques sans que vous ayez à intervenir. Maintenez vos logiciels à jour, préférez les messageries chiffrées de bout en bout qui ont annoncé une migration PQC, et gardez à l'esprit qu'une donnée qui doit rester secrète pendant vingt ans ne devrait pas transiter aujourd'hui sur un canal chiffré uniquement en RSA.

Si vous pilotez un système d'information

Là, le travail est réel et il a déjà commencé ailleurs. Le premier geste n'est pas de choisir un algorithme, mais de savoir ce que l'on a. L'inventaire cryptographique est décrit par tous les référentiels comme l'étape fondatrice, et c'est aussi la plus longue.

Dresser l'inventaire cryptographique. Pas une liste de certificats : une cartographie des algorithmes, des clés, des certificats, des dépendances tierces, des bibliothèques embarquées, des équipements réseau et des cartes à puce.

Identifier les données à durée de vie longue. Toute donnée qui doit rester confidentielle au-delà de 2035 est déjà exposée au scénario de moisson anticipée. Dans le monde universitaire et hospitalier, cela couvre les dossiers de recherche, les données de santé, les données RH et les archives administratives.

Interroger les fournisseurs sur leur feuille de route PQC. Un équipement acheté aujourd'hui pour dix ans doit être crypto-agile, c'est-à-dire capable de changer d'algorithme par mise à jour. C'est une clause de marché, pas une option technique.

Prioriser les usages à risque élevé. Les référentiels français ciblent 2030 pour la migration des systèmes critiques et 2035 pour la généralisation.

Privilégier les mécanismes hybrides. L'ANSSI recommande de combiner un algorithme classique éprouvé et un algorithme post-quantique : on ne perd rien en sécurité actuelle et on gagne la protection future, ce qui est la position raisonnable tant que les nouveaux algorithmes n'ont pas vieilli.

Former, sensibiliser, gouverner. Le sujet croise la sécurité, les achats, l'architecture et la conformité. Sans porteur identifié, il ne se passe rien pendant trois ans, puis tout devient urgent.

Si vous êtes dans un secteur applicatif

Chimie, pharmacie, énergie, finance, logistique, défense : le bon niveau d'engagement en 2026 n'est ni l'achat d'une machine ni l'indifférence. C'est l'identification interne de deux ou trois problèmes candidats, et l'accès via le cloud à des QPU pour tester des prototypes. C'est exactement ce que fait la majorité des trois cents entreprises recensées comme actives sur le sujet : elles construisent des compétences et des cas d'usage, pas des salles machines.

Conclusion

L'informatique quantique n'est pas une technologie de demain, et elle n'est pas non plus la révolution imminente que certaines annonces laissent entendre. Elle est dans cet entre-deux inconfortable où la physique est validée, l'ingénierie encore fragile, l'économie déjà bruyante.

Ce qui s'est passé en décembre 2024 est réel : un verrou théorique vieux de trente ans a sauté. Ce qui se passe depuis est une course industrielle et géopolitique dont les jalons sont désormais datés et vérifiables — fin 2026 pour l'avantage quantique annoncé par IBM, 2029 pour les premiers systèmes

tolérants aux fautes, 2030 à 2035 pour la fenêtre du Q-Day.

Et il y a une conséquence qui n'attend aucun de ces jalons. La migration cryptographique mondiale a commencé, ses échéances sont écrites, et le scénario de la moisson anticipée fait que le retard pris aujourd'hui ne se rattrape pas : une donnée interceptée en 2026 et déchiffrée en 2035 ne peut pas être re-protégée rétroactivement.

Comprendre ce qui se construit dans ces laboratoires refroidis à quelques millièmes de degré au-dessus du zéro absolu, c'est comprendre dans quel monde numérique on vivra dans dix ans. Et pour une fois, la partie la plus urgente du sujet ne demande pas d'attendre : elle demande un inventaire.
