Transition post-quantique : état des lieux 10 ans après l'annonce choc de la NSA

Par Simon ABELARD
Enseignant-chercheur à l'EPITA
(École pour l'Informatique et les Techniques avancées)

Et Ludovic PERRET
Professeur à l'EPITA

Si l'on sait depuis 1994 que l'ordinateur quantique menace les méthodes de chiffrement actuelles, cette menace ne s'est véritablement matérialisée qu'en 2015 à l'appel d'institutions américaines telles que la NSA et le NIST. Dix ans plus tard, il est temps de faire un bilan sur la réalité de la menace quantique, sur les efforts mis en place des deux côtés de l'Atlantique et sur le chemin qu'il reste à parcourir. À première vue, on pourrait craindre que l'Europe soit en retard sur le sujet mais nous proposons une analyse plus fine des forces et des faiblesses du Vieux Continent.

Remerciements
Les auteurs souhaitent remercier Christopher Bonnelly pour sa lecture attentive et ses remarques sur l'article, ainsi que Daniel Boula et Grégoire Postel-Vinay pour leurs commentaires.

Introduction

L'année 2025 marque le début de la transition à grande échelle des infrastructures numériques vers une cryptographie de nouvelle génération, dite cryptographie post-quantique (Fouque, Lafourcade et Perret, 2026), conçue pour résister aux attaques quantiques.

Cette transition s'amorce exactement dix ans après une annonce de la NSA (National Security Agency) américaine, publiée[1] pendant l'été 2015. Les progrès des ordinateurs quantiques remettraient en cause la sécurité à long terme des algorithmes cryptographiques à clé publique classiques, tels que le protocole d'échange de clés de Diffie-Hellman ou le chiffrement RSA.

L'annonce est surprenante et son impact potentiellement colossal puisque la sécurité d'Internet et des communications numériques reposent en grande partie sur ces deux cryptosystèmes, massivement déployés à l'échelle mondiale depuis les années 1980.

Depuis les travaux de Peter Shor (Shor, 1994), nous savons que les ordinateurs quantiques pourraient théoriquement casser ces deux problèmes mathématiques, la factorisation des

[1] https://arstechnica.com/information-technology/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/

grands entiers et le calcul du logarithme discret, sur lesquels reposent respectivement la sécurité de RSA et de Diffie-Hellman. Certes, les résultats de Shor rendent obsolètes les mécanismes de sécurité classiques, mais cette menace, connue de longue date, n'était pas perçue comme critique en raison des capacités très limitées des ordinateurs quantiques de l'époque.

Malgré tout, cette annonce de la NSA a déclenché une mobilisation internationale impliquant, entre autres, des organismes de normalisation, des agences de sécurité, et de nombreux acteurs du monde académique et industriel.

Le résultat le plus visible est le processus de normalisation de la cryptographie post-quantique (Chen *et al.*, 2016) entamé en 2016 par l'institut américain NIST (National Institute of Standards and Technology). Ce processus s'est achevé en 2025 avec la normalisation de cinq nouveaux algorithmes divisés en deux catégories : l'échange de clés, avec deux algorithmes, et la signature, avec trois algorithmes.

Ces algorithmes reposent sur des problèmes et principes mathématiques différents de ceux de RSA et de Diffie-Hellman. Les réseaux euclidiens, les matrices et les polynômes y remplacent les groupes finis, courbes elliptiques et entiers modulaires. En revanche, ces nouveaux cryptosystèmes s'utilisent de la même manière que les anciens, et l'utilisateur final n'y verra (presque) aucune différence.

Les contributions françaises et européenne au processus post-quantique du NIST sont remarquables : quatre des cinq algorithmes normalisés par le NIST ont été co-inventés par des chercheurs travaillant dans des écoles d'ingénieurs ou des universités françaises. Ce pourcentage atteint même 100 % lorsque l'on inclut les contributeurs issus d'institutions européennes. Les travaux préliminaires ayant conduit à ces résultats ont souvent été financés par des fonds publics, notamment par le biais de l'ANR (Agence Nationale pour la Recherche), de BPI France et de fonds européens dédiés à la recherche et à l'innovation.

Dix ans après l'annonce de la NSA, cet article propose un bilan de l'état actuel de la menace quantique, aborde les prochains défis de la cryptographie post-quantique et propose une mise en perspective des stratégies européenne et américaine dans ce domaine. L'Europe sera-t-elle au rendez-vous de la transition post-quantique ?

Menace quantique sur la cryptographie

Si, en 2015, la menace quantique semblait encore lointaine, voire relever de la science-fiction, les progrès accomplis ces dernières années dans le développement des ordinateurs quantiques sont impressionnants : revendication de la « suprématie quantique[2] » par Google en 2019, progrès constants d'IBM, qui suit une feuille de route technologique rendue publique depuis plusieurs années[3], et machines aux capacités croissantes à travers le monde, notamment en Australie, au Canada, en Chine, au Japon, au Royaume-Uni, aux États-Unis, et en Europe, qui n'est pas en reste dans cette course technologique. En 2025, la Commission européenne recensait 39 *start-ups* cherchant à construire un ordinateur quantique (Com, 2025), dont 4 en France.

Un moyen simple d'évaluer les capacités de calcul d'un ordinateur quantique est de compter le nombre de *qubits*, l'équivalent quantique du bit classique. Ce seul critère ne suffit pas à rendre compte de la puissance réelle des machines quantiques actuelles. En effet, les *qubits* sont extrêmement sensibles aux perturbations, ce qui engendre des erreurs et limite leurs performances.

[2] https://www.nature.com/articles/s41586-019-1666-5

[3] https://www.ibm.com/quantum/technology#roadmap

Il convient alors de distinguer les *qubits* dits « logiques », qui sont des *qubits* théoriquement parfaits et auto-corrigés, des *qubits* « physiques », qui, eux, sont sujets à des erreurs et possèdent un temps de cohérence (la durée avant que les erreurs ne se produisent) limité. Habituellement, les communications reliées à la puissance des ordinateurs quantiques correspondent aux *qubits* logiques.

Cependant, une augmentation du nombre de *qubits* logiques n'implique pas nécessairement une amélioration des capacités de calcul. Par exemple, la feuille de route d'IBM annonce 120 *qubits* pour 2025, alors qu'une machine de 156 *qubits* était déjà disponible dès 2024. Après une première phase dédiée à l'augmentation du nombre de *qubits* (par exemple, 5 *qubits* en 2016), IBM semble désormais se concentrer sur l'amélioration de la qualité plutôt que de la quantité[4]. Le nombre de *qubits* est une mesure d'autant plus imparfaite qu'il existe de multiples technologies présentant chacune des avantages et des inconvénients, de sorte que tous les *qubits* ne se valent pas.

Briser la sécurité des algorithmes cryptographiques déployés actuellement nécessiterait la construction d'un ordinateur quantique de grande capacité, doté d'un nombre bien plus élevé de *qubits*. À titre d'exemple, examinons les ressources nécessaires pour factoriser un entier RSA-2048, une clé RSA de 2 048 bits, taille typique de paramètre utilisé en pratique. Avec des machines classiques, il faudrait mobiliser des milliers de supercalculateurs pendant plusieurs siècles pour casser RSA-2048. Ce même calcul ne prendrait que quelques minutes sur une machine quantique, à condition de disposer de 1 399 *qubits* logiques.

En l'état actuel des connaissances, il faudrait environ 1 million de *qubits* physiques pour réaliser ce calcul en quelques heures (Gidney, 2025). Cette dernière évaluation prend en compte des progrès dans l'amélioration de la qualité des *qubits* (Google AI *et al.*, 2024), mais surtout des avancées algorithmiques récentes sur l'algorithme de Shor (Chevignard, Fouque et Schrottenloher, 2024) qui ont permis de réduire significativement les ressources nécessaires pour effectuer ce même calcul. En effet, en 2019, les auteurs (Gidney et Ekerå, 2021) estimaient qu'environ 20 millions de *qubits* logiques seraient nécessaires pour casser RSA-2048.

La marge de progression reste donc encore très significative avant d'obtenir une machine quantique capable de briser la cryptographie actuelle. Cependant, les progrès réalisés ces dernières années sont considérables, tant sur le plan matériel qu'algorithmique.

Au-delà de ces aspects scientifiques et technologiques, les investissements réalisés à travers le monde pour la construction d'un ordinateur quantique de grande capacité sont importants et s'élèvent à plusieurs milliards en Europe, en Chine ou aux États-Unis. Au niveau national, le programme PROQCIMA[5], porté par le ministère des Armées et France 2030, est doté d'un budget de 500 millions d'euros et ambitionne de construire un ordinateur quantique de 128 *qubits* logiques en 2032 et 2 048 *qubits* logiques en 2035, machine qui serait notamment capable de briser RSA-2048.

Ces objectifs sont ambitieux et montrent que l'incertitude ne porte pas tant sur la capacité à construire une machine de grande envergure que sur le délai nécessaire pour y parvenir. Le rapport très complet du BSI (2024), l'agence de sécurité allemande, estime, d'une part, que l'arrivée d'un ordinateur quantique de grande capacité interviendra au plus tard en 2040 et, d'autre part, que la plupart des obstacles techniques ont été levés en 2024.

[4] Le lecteur intéressé par des précisions pourra consulter le très complet et détaillé panorama des technologies quantiques (Ezratty, 2024).

[5] https://quantique.france2030.gouv.fr/acces-aux-marches/programme-proqcima/

Cette menace peut malgré tout sembler lointaine, mais elle pèse déjà sur les communications les plus sensibles. En effet, il est d'ores et déjà possible de capturer et de stocker des données chiffrées à grande échelle, en attendant qu'un ordinateur quantique suffisamment puissant soit disponible pour en révéler les secrets. Les objets connectés à longue durée de vie, comme les voitures connectées, les avions, les satellites ou les systèmes d'armes modernes sont également concernés. Déployés pour plusieurs décennies, ils ne disposent souvent d'aucun moyen simple permettant de mettre à jour leurs composants cryptographiques.

Une stratégie américaine constante et structurée

L'objectif de transition vers le post-quantique fixé par la NSA en 2015 n'a pas bougé au fil des années et s'est structuré autour de trois grandes phases. Le processus de normalisation du post-quantique du NIST, mentionné dans l'introduction, constitue la première étape qui s'est achevée en 2025. Cela ne signifie pas pour autant que les activités de normalisation post-quantique sont terminées. Elles se poursuivent sous d'autres formes au sein d'organismes comme l'ETSI, l'IETF ou l'ISO, principalement pour intégrer les normes du NIST dans divers protocoles de sécurité à l'échelle mondiale.

La deuxième phase, officiellement démarrée en 2023, consiste à accompagner les industriels dans la transition post-quantique. Cet accompagnement prend la forme d'un partenariat public-privé au sein du NCCoE[6], laboratoire du NIST qui rassemble plusieurs agences américaines et des acteurs industriels. Dès aujourd'hui, les acteurs américains affichent un niveau de maturité élevé, puisque des entreprises comme AWS, Apple, ou Google ont intégré des solutions post-quantiques dans certaines de leurs offres grand public (navigateur Chrome post-quantique, iMessage post-quantique, ou plateforme d'accès post-quantique au *cloud* AWS). Ces acteurs ne représentent certes pas l'intégralité du paysage économique américain, mais il est indéniable que leur poids suffit à tirer tout l'écosystème vers le haut.

La troisième phase concerne la régulation, avec une loi fixant à 2035 la date limite pour la transition des infrastructures numériques publiques vers le post-quantique (WH, 2025), un schéma de certification des produits de cybersécurité adapté au post-quantique (CMVP, FIPS 203/204) et la dépréciation programmée des normes non résistantes aux attaques quantiques d'ici 2035. Dans (Moody *et al.*, 2025), le NIST indique que des algorithmes comme RSA et Diffie-Helmman ne seront plus acceptés après 2035.

L'Europe à l'heure du post-quantique ?

Malgré l'excellence scientifique de ses chercheurs et de ses universités, l'Europe a quelque peu tardé à se saisir des problématiques politiques et organisationnelles liées à la transition vers la cryptographie post-quantique. On peut, par exemple, s'interroger sur l'absence de contrepartie européenne à la campagne de normalisation du NIST, *a fortiori* quand d'autres acteurs comme la Chine et la Corée du Sud ont lancé leurs propres campagnes.

La France est partie prenante des travaux en cours sur la normalisation du post-quantiques et s'implique activement dans des organismes comme l'IETF, l'ETSI ou lISO, notamment par l'intermédiaire de l'AFNOR, qui coordonne les contributions des acteurs français. Cependant, cette stratégie d'influence reste bien moins développée que celles

[6] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

déployées par les Américains, les Britanniques ou les Chinois, qui y consacrent des moyens considérables. Cet état de fait n'est pas anodin car l'adoption ou la non-adoption de normes peut se révéler très impactante pour les industriels.

Le constat est similaire au niveau de l'Union européenne. Pour autant, il serait faux de croire que l'Europe n'a rien fait en la matière : scientifiquement parlant, l'Europe n'a pas tardé, puisqu'elle a lancé, entre autres, les projets de recherche ECRYPT-CSA[7] et PQCRYPTO[8] dès 2015, projets qui seront suivis par de nombreux autres. Il est également important de noter que les universitaires se sont saisis du problème en intégrant très rapidement les enjeux du quantique dans les formations, comme la majeure quantique de l'EPITA[9], les masters d'informatique quantique de Sorbonne Université (QI[10]), l'Institut Polytechnique (QMI[11]), etc. L'Europe anticipe également la question des normes puisque l'ETSI a créé un groupe dédié au post-quantique qui produit régulièrement des spécifications.

Dès 2021, l'ENISA a rédigé des rapports sur la cryptographie post-quantique (D'Anvers *et al.*, 2021 ; Bernstein *et al.*, 2022) et sur son intégration (performances, protocoles, hybridation, normalisation). Ces rapports sont cependant essentiellement techniques et ne contiennent que peu de recommandations. Peu après, les agences française et allemandes (ANSSI 22 ; Ehlen *et al.*, 22) ont publié des recommandations sur le choix des algorithmes cryptographiques et plus généralement sur la transition vers le post-quantique. Si on peut saluer le fait que les deux agences partagent une vision très similaire, il n'est pas encore question à l'époque de position commune à l'échelle européenne.

Il faudra attendre avril 2024 pour que la Commission européenne publie une recommandation (EC, 2024) suivie en 2025 d'une feuille de route concernant la transition vers le post-quantique (NIS, 2025) dont les principes fondamentaux sont les suivants :

- Jalons : travaux initiés, et feuille de route de transition post-quantique avant fin 2026 par les agences nationales, transition effectuée avant 2030 pour les applications sensibles et avant 2035 pour les autres applications.
- Modalités : opter pour des solutions hybrides et garantir la crypto-agilité, c'est-à-dire la possibilité de changer d'algorithme cryptographique sans modification du matériel ou des protocoles. Ces deux exigences visent à anticiper l'éventualité qu'un algorithme post-quantique soit cassé (cela s'est produit lors de la campagne du NIST), ou que son implémentation ne soit pas sûre.
- Écosystème : s'assurer que l'Europe dispose de formations de haut niveau en cryptographie post-quantique, définir des critères communs pour la certification de la cryptographie post-quantique et pour l'évaluation du risque quantique, et se doter d'un organe de communication concernant l'impact du quantique.

Cette publication un peu tardive d'une feuille de route illustre que les défis de la transition ne résident pas seulement dans les aspects technologiques, mais aussi dans les dimensions organisationnelles – avec notamment un besoin crucial de coordination (QSFF, 2024 ; Perret et Ribordy, 2025) entre de nombreux acteurs (agences de sécurité, acteurs de la normalisation, régulateurs, industriels, académiques, etc.).

[7] https://cordis.europa.eu/project/id/645421/reporting

[8] https://pqcrypto.eu.org/

[9] https://www.epita.fr/ecole-ingenieurs/informatique-et-technologies-quantiques/

[10] https://qics.sorbonne-universite.fr/formation/programme-de-master

[11] https://quriosity.telecom-paris.fr/qmi/courses.html

À l'échelle industrielle, si les géants de la tech américaine n'ont pas attendu pour être proactifs dans le développement et la transition vers des solutions post-quantiques, les grands industriels européens ne se sont pas encore suffisamment saisis du sujet, à l'exception notable des acteurs visant le marché de la défense ou celui des opérateurs d'importance vitale. On peut citer par exemple Atos et Thales qui ont tous les deux annoncé des versions de leurs modules de sécurité (HSM) supportant les algorithmes post-quantiques standardisés par le NIST.

On peut nuancer ce constat en remarquant le nombre important de *start-ups* proposant des services ou des bibliothèques logicielles pour soutenir la transition vers le post-quantique. Ces acteurs ont une expertise solide et reconnue, mais il est toutefois peu probable que leur petit nombre suffise à couvrir les énormes besoins du marché européen.

Dans la transition vers le post-quantique, l'Europe peut compter sur ses nombreux experts mais il est désormais temps pour elle de transformer l'essai en développant une politique industrielle (D'Auria *et al.*, 2025) aussi claire, harmonieuse et volontariste que celle menée outre Atlantique. S'il ne faut pas s'alarmer de l'absence de campagne de normalisation européenne analogue à celle du NIST, il faut s'assurer que les acteurs européens publics et privés auront des lignes de conduite claires et un accompagnement suffisant pour les mettre en œuvre.

Cela motive certaines institutions européennes à promouvoir des actions sectorielles afin de mettre en place des stratégies adaptées, c'est par exemple le cas dans le secteur financier avec la mise en place, par Europol en 2024, du Quantum Safe Financial Forum (QSFF, 2024), une initiative qui va au-delà des frontières européennes puisqu'elle regroupe également des acteurs britanniques et américains. À plus long terme, il serait souhaitable que l'Europe reprenne un rôle de leader en lançant des travaux de normalisation des protocoles cryptographiques. De nombreuses opportunités restent à saisir dans le domaine : 5G, 6G, standards du CCSDS dans le spatial, etc.

Enfin, le volontarisme américain dans le domaine du post-quantique contraste fortement avec leur peu d'engouement pour la cryptographie quantique. Pourtant, cette dernière offre une approche alternative, permettant en théorie de garantir une sécurité inconditionnelle face aux attaques d'un ordinateur quantique. En revanche, la cryptographie quantique nécessite la mise en place d'une nouvelle infrastructure et se heurte encore à des limitations fortes (absence d'authentification, distance limitée, forte dépendance au matériel employé, faiblesse face aux dénis de service, etc.) soulignées par la NSA et également par plusieurs agences européennes (ABNS, 2024).

Cependant, cela laisse pour le moment une place pour un écosystème quantique européen, avec notamment l'initiative EuroQCI[12] menée par la Commission européenne qui regroupe à la fois des infrastructures terrestres et spatiales. Malgré la relative absence des États-Unis dans ce domaine, la concurrence sera rude, principalement avec la Chine, qui bat de nombreux records et fait figure de *leader* dans le domaine. L'espoir est toutefois permis car l'Europe a pleinement compris que la révolution quantique est un tournant historique dans la compétition économique et géostratégique mondiale, comme en témoigne l'axe quantique du projet EuroHPC[13] Joint Undertaking visant à exploiter des puces quantiques dans le domaine des supercalculateurs et le "Quantum Act" actuellement en préparation (Com, 2025).

[12] https://digital-strategy.ec.europa.eu/fr/policies/european-quantum-communication-infrastructure-euroqci

[13] https://www.eurohpc-ju.europa.eu/eurohpc-quantum-computers_en

Bibliographie

(ABNS, 2024) – ANSSI, BSI, NLNCSA, NCSA (2024), "Position paper on quantum key distribution", https://cyber.gouv.fr/actualites/uses-and-limits-quantum-key-distribution

(ANSSI, 2022) – AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (2022), "ANSSI views on the post-quantum cryptography transition", https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

(Bernstein *et al.*, 2022) – BERNSTEIN D. J., HÜLSING A., LANGE T. & REKLEITIS E. (2022), "Post-quantum cryptography – Integration study", ENISA, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2824/151162

(BSI, 2024) – FEDERAL OFFICE FOR INFORMATION SECURITY, BSI (2024), "The status of quantum computer development", https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html?nn=916616

(Chen *et al.*, 2016) – CHEN L., JORDAN S., LIU Y.-K, MOODY D., PERALTA R., PERLNER R. & SMITH-TONE D. (2016), "Report on post-quantum cryptography standards", NIST IR 8105, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

(Chevignard, Fouque & Schrottenloher, 2024) – CHEVIGNARD C., FOUQUE P.-A. & SCHROTTENLOHER A. (2025), "Reducing the number of qubits in quantum factoring", Crypto 2025, https://eprint.iacr.org/2024/222

(Com, 2025) – COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL (2025), "Quantum Europe strategy: Quantum Europe in a changing world", COM (2025), 363 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0363

(D'Anvers *et al.*, 2021) – D'ANVERS J.-P., HÜLSING A. LANGE T., PANNY L., DE SAINT GUILHEM C. & SMART N. P. (2021), "Post-quantum cryptography – Current state and quantum mitigation", ENISA, Publications Office of the European Union, https://data.europa.eu/doi/10.2824/92307

(D'Auria *et al.*, 2025) – D'AURIA V., CHRISTOFI M., EALET F., FUNKE J.-F., KÉNANIAN G., LOIDREAU P., LAURENT E., PERRET L., SENOT O., TELLER M. & VILLARD A. (2025), « Cryptographie post-quantique : quelle stratégie industrielle ? », *Dalloz IP/IT*.

(EC, 2024) – COMMISSION RECOMMENDATION (EU) 2024/1101 (2024), "Recommandation on a coordinated implementation roadmap for the transition to post-quantum cryptography", https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

(Ehlen *et al.*, 2022) – EHLEN S, HAGEMEIER H, HEMMERT T, KOUSIDIS S, LOCHTER MANFRED, REINHARDT S. & WUNDERER T. (2022), "Quantum-safe cryptography – fundamentals, current developments and recommendations", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4

(Ezratty, 2024) – EZRATTY O. (2024), "Understanding quantum technologies 2024", https://www.oezratty.net/wordpress/2024/understanding-quantum-technologies-2024/

(Fouque, Lafourcade & Perret, 2026) – FOUQUE P.-A., LAFOURCADE P. & PERRET L. (2026), *Cryptographie Post-Quantique*, Dunod (à paraître).

(Gidney et Ekerå, 2025) – GIDNEY C. & EKERÅ M. (2021), "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", *Quantum*, Vol. 5, https://arxiv.org/abs/1905.09749

(Gidney, 2025) – GIDNEY C. (2025), "How to factor 2048 bit RSA integers with less than a million noisy qubits", ePrint arXiv:2505.15917, https://arxiv.org/abs/2505.15917

(Google AI *et al.*, 2024) – GOOGLE QUANTUM AI & COLLABORATORS (2025), "Quantum error correction below the surface code threshold", *Nature*, Vol. 638, https://www.nature.com/articles/s41586-024-08449-y

(Moody *et al.*, 2025) – MOODY D., PERLNER R., REGENSCHEID A., ROBINSON A. & COOPER D. (2024), "Transition to post-quantum cryptography standards", NIST IR 8547, https://doi.org/10.6028/NIST.IR.8547.ipd

(NIS, 2025) – NIS COORDINATION GROUP (2025), "A coordinated implementation roadmap for the transition to post-quantum cryptography", https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

(Perret et Ribordy, 2025) – PERRET L. & RIBORDY G. (2025), "Accelerating the transition to quantum-safe communication: A call for global collaboration and action", Policy brief, G7 Kananaskis, Think7 Canada 2025, https://www.think7.org/publications/accelerating-the-transition-to-quantum-safe-communication-a-call-for-global-collaboration-and-action/

(QSFF, 2024) – EUROPEAN CYBERCRIME CENTRE (EC3), EUROPOL (2024), "Quantum safe financial forum: a call to action", doi:10.2813/5052685, https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action

(Shor, 1994) – SHOR P. W. (1994), "Algorithms for quantum computation: Discrete logarithms and factoring", FOCS 1994.

(WH, 2025) – WHITE HOUSE (2025), "National security memorandum on promoting United States leadership in quantum computing while mitigating risks to vulnerable cryptographic systems", https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/