Cryptographie post-quantique

Pierre-Alain FOUQUE
Pascal LAFOURCADE
Ludovic PERRET

Préface de David Pointcheval

DUNOD

Direction et conception graphique de la couverture :
Nicolas Wiel – Elizabeth Riba (graphiste)

11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-085584-1

Préface

Les avancées majeures autour de l'ordinateur quantique font régulièrement la une des journaux avec, en ligne de mire, la « suprématie quantique » et la démonstration qu'un ordinateur quantique peut résoudre un problème hors de portée des ordinateurs classiques. Le nombre croissant de qubits offerts par les nouveaux ordinateurs quantiques promet de révolutionner l'approche de tous les problèmes d'optimisation, avec des retombées importantes dans de nombreux domaines technologiques, tels que la chimie ou l'intelligence artificielle. Cependant, l'avènement potentiel de ces technologies présente également un défi pour la sécurité de nos systèmes d'information. Bien avant sa conception pratique, la communauté informatique a modélisé les capacités d'un tel ordinateur quantique. Ont alors été proposés des algorithmes exploitant ses nouvelles propriétés, telles que l'intrication et la superposition quantiques. En particulier, les algorithmes de Shor et de Grover, publiés dans les années 1990, ont des applications immédiates en théorie des nombres et sur les fonctions à sens unique, qui sont les fondements de la cryptographie actuelle. Ainsi, les algorithmes cryptographiques classiques pour la confidentialité, l'intégrité et l'authentification des données, qui ont sécurisé le web et les infrastructures numériques pendant des décennies, se voient remis en question par ces nouvelles capacités de calcul, mais de façon très variable. Cet ouvrage propose un parcours clair et rigoureux au cœur de la cryptographie post-quantique, pour comprendre les enjeux et les menaces d'un potentiel ordinateur quantique, sans les dramatiser, puis en présentant les alternatives candidates capables de résister aux éventuelles attaques quantiques. Il fournit, aux lectrices et lecteurs, toutes les clés pour bien appréhender la transition post-quantique.

En effet, la menace quantique n'est pas immédiate, avec des impacts très variables selon les cas d'usage, mais elle est bien réelle et il est crucial de s'y préparer dès aujourd'hui. Le slogan *harvest now, decrypt later*, ou « récolter maintenant, décrypter plus tard », illustre bien le risque que des données sensibles aujourd'hui protégées par des mécanismes classiques puissent être compromises dans le futur, lorsque des ordinateurs quantiques suffisamment puissants seront disponibles. Malheureusement, aucune direction technique unique n'émerge encore clairement, déjà sur les choix des solutions post-quantiques, mais également sur les approches « hybrides » ou « pures post-quantiques ». Néanmoins, plusieurs familles de solutions prometteuses ont été identifiées, et les organismes de normalisation jouent leur rôle. En revanche, profiter de cette migration pour revoir les architectures de sécurité, améliorer la gestion des clés et renforcer la crypto-agilité est une opportunité à saisir, qui fait consensus. Dans ce contexte, la transition doit être anticipée avec pragmatisme et discernement.

La force et la justesse de ce livre tiennent à la complémentarité de ses auteurs, tous trois professeurs spécialistes de cryptographie. Plus particulièrement, Pierre-Alain Fouque est professeur à l'Université de Rennes. Ses travaux portent sur la cryptographie post-quantique et ses applications, avec une attention aux aspects de normalisation et d'implémentation. Pascal Lafourcade est professeur à l'Université Clermont Auvergne, où il contribue à l'enseignement et à la recherche sur les réseaux et la sécurité, et excelle dans la vulgarisation scientifique de ces sujets complexes. Ludovic Perret est professeur à l'EPITA. Son expertise en sécurité des systèmes et son expérience en ingénierie complètent les perspectives proposées dans cet ouvrage, notamment sur les aspects de migration post-quantique.

J'en profite pour les remercier chaleureusement pour la confiance qu'ils m'ont accordée pour écrire cette préface. Cela me permet de souligner la qualité de leur travail, qui allie rigueur scientifique, clarté pédagogique et sens des enjeux d'implémentation et de normalisation. Par leur expertise, ils éclairent avec justesse le contexte, les enjeux et les perspectives de la transition post-quantique qui se met en place.

Ce livre s'adresse à un public large mais exigeant, notamment aux étudiants, mais également aux praticiens (ingénieurs, architectes ou responsables sécurité). Un bagage standard en mathématiques sera nécessaire, mais des exemples et des exercices (avec corrigés) accompagnent le lecteur. Puis des encadrés proposent aux plus curieux des compléments pour aller plus loin. Le contenu est développé en trois étapes, avec un niveau de technicité adapté à chacun des sujets. Il commence par expliquer le contexte et ses enjeux : rappel de la cryptographie moderne, avec les modèles de sécurité, et comment les algorithmes de Shor et de Grover rebattent les cartes, en précisant les menaces réelles et les échéances probables. Vient ensuite le sujet des réponses opérationnelles appropriées, avec la transition post-quantique et les recommandations des organismes de normalisation. Enfin, le livre entre plus en détail dans les différentes familles de primitives post-quantiques : constructions, analyses de sécurité et performances. Des compléments mathématiques décrivent tous les outils mis en œuvre, ainsi que les notions nécessaires pour bien comprendre les mécanismes post-quantiques. Chaque chapitre propose des exemples, des schémas, des références commentées et des exercices à difficulté graduée. Ce livre fait également le lien entre la théorie et la pratique en précisant la complexité et en fournissant un paramétrage concret des solutions évoquées.

Les auteurs proposent donc un texte accessible et précis, avec les notions essentielles, le contexte des résultats et les points d'attention concrets pour la prise de décision technique. Ils mettent en évidence les limites et incertitudes connues, et indiquent les pistes de recherche actives afin de guider la veille technologique. Ce livre aidera ses lectrices et lecteurs — étudiantes, étudiants, ingénieures, ingénieurs et praticiens — à comprendre les enjeux, à évaluer les solutions et à engager, pas à pas, la transition vers des mécanismes cryptographiques capables de résister à l'ère quantique.

À Paris, le 15 janvier 2026.
David Pointcheval - directeur scientifique de Cosmian,
Médaille d'argent 2021 du CNRS et
Prix Lazare Carnot 2025 de l'Académie des Sciences.

Avant-propos

Le XXI^{e} siècle est celui de la cryptographie avancée et des nouveaux problèmes mathématiques résistants à l'ordinateur quantique. La cryptographie post-quantique, plus résistante, introduit aussi des cryptosystèmes dotés de nouvelles fonctionnalités, comme le chiffrement homomorphe, amenant la cryptographie dans une nouvelle ère. En effet, en 2016, le processus de normalisation dédié à la cryptographie post-quantique est initié par le très influent organisme américain *National Institute of Standards and Technology* (NIST). Après plusieurs années de travail intensif, en collaboration avec la communauté internationale, le NIST publie entre 2022 et 2025 les premières normes de cryptographie post-quantique. Compte tenu de cette normalisation, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande, dès à présent, de démarrer la migration vers le post-quantique. Par conséquent, l'ensemble de la filière cybersécurité va devoir intégrer ces nouvelles normes pour garantir la sécurité de nos données sur le long terme.

Cet ouvrage est un livre de cours, illustré par des exercices corrigés, dont l'objectif est d'expliquer les fondements de la cryptographie post-quantique en se concentrant sur les nouvelles normes du domaine. L'ouvrage s'adresse à des étudiants de second cycle d'informatique ou de mathématiques, aux élèves ingénieurs ainsi qu'aux ingénieurs R&D en cybersécurité qui souhaitent se former sur la cryptographie post-quantique.

Le premier chapitre explique pourquoi l'arrivée de l'ordinateur quantique va impacter la sécurité de nombreuses primitives cryptographiques de notre quotidien. Le second chapitre introduit les concepts fondamentaux de la cryptographie. Le chapitre suivant présente le calcul quantique et les algorithmes quantiques qui impactent la cryptographie pré-quantique. Dans le quatrième chapitre, la question de la transition post-quantique est abordée. Dans le cinquième chapitre, les algorithmes de signature post-quantique reposant sur les fonctions de hachage sont décrits. Dans le sixième chapitre, les primitives sur les codes sont présentées. Les chiffrements et signatures à base de réseaux euclidiens sont abordés dans le septième chapitre. Les derniers chapitres présentent des compléments sur les réseaux euclidiens, des rappels de mathématiques et les solutions des exercices.

Les auteurs expriment leur gratitude à S. Abelard, O. Allabwani, N. Aragon, O. Blazy, M. Bombardelli, A. Carapostol, T. Cauët-Male, M. Daniel, N. Gurel, G. De Julis, A. Graingnic, T. Lopez, P. Lacome, C. Olivier-Anclin, D. Sow, T. Ricosset, B. Vulpescu pour leurs commentaires, suggestions et relectures assidues.

À Rennes, Clermont-Ferrand et Paris, le 19 janvier 2026.

Pierre-Alain Fouque, Pascal Lafourcade et Ludovic Perret.

À nos femmes.

Table des matières VII

Notations

Le tableau ci-dessous liste les notations utilisées dans cet ouvrage.

$\{0,1\}^n$	Ensemble des chaînes binaires de longueur n
$\{0,1\}^*$	Ensemble des chaînes binaires de longueur quelconque
$\#E$	Nombre d'éléments de l'ensemble E
$\mathbb{Z}$	Ensemble des entiers relatifs
$\mathbb{Z}_{>n}$	Ensemble des entiers relatifs strictement plus grand que n
$\mathbb{Z}_N^\times$	Ensemble des éléments inversibles modulo N
$\mathbb{Q}$	Ensemble des nombres rationnels
$\mathbb{R}$	Ensemble des nombres réels
$\mathbb{C}$	Ensemble des nombres complexes ou imaginaires
$\overline{z}$	Conjugué du nombre complexe z
$\lvert z\rvert$	Norme du nombre complexe z
$\mathbb{F}_p$	Corps fini à p éléments
$\mathbb{F}_p[X_1,\ldots,X_n]$	Ensemble des polynômes en n variables à coefficients dans $\mathbb{F}_p$
$\mathbf{A}$	Les matrices sont notées en gras en majuscule
$\mathbf{a}$	Les vecteurs sont notés en gras en minuscule
$\hat{\mathbf{a}}$	Vecteur de la transformée de Fourier du polynôme $a(X)$
$\lVert\mathbf{x}\rVert_1$	Norme L_1 du vecteur $\mathbf{x}$
$\lvert\psi\rangle$	Un qubit
$\mathbf{A}\lvert\mathbf{B}$	Concaténation des matrices $\mathbf{A}$ et $\mathbf{B}$
$\mathbf{x} \mid\mid \mathbf{y}$	Concaténation de deux chaînes binaires $\mathbf{x}$ et $\mathbf{y}$
$\mathbf{x} \oplus \mathbf{y}$	XOR (ou exclusif bit à bit) de $\mathbf{x}$ et $\mathbf{y}$
$\langle\mathbf{u},\mathbf{v}\rangle$	Produit scalaire entre les vecteurs $\mathbf{u}$ et $\mathbf{v}$
$\mathbf{x} \otimes \mathbf{y}$	Produit tensoriel de $\mathbf{x}$ et $\mathbf{y}$
$\mathbf{a} \circ \mathbf{b}$	Multiplication dans $\mathbb{Z}_q$ coordonnée à coordonnée de $\mathbf{a}$ et $\mathbf{b}$
$\Pr[A]$	Probabilité de l'événement A
$x \in_R S$	x est choisi uniformément dans l'ensemble S
$\lfloor x \rfloor$	Partie entière inférieure de x
$\lceil x \rceil$	Partie entière supérieure de x
$\lceil x \rfloor$	Arrondi de x à l'entier le plus proche
$x \ll y$	x est beaucoup plus petit que y
$x \gg y$	x est beaucoup plus grand que y
$n!$	Factorielle de n qui vaut $1 \cdot 2 \cdot \ldots n$
$\varphi(n)$	Indicatrice d'Euler de l'entier n
$\mathrm{pgcd}(a,b)$	Plus grand commun diviseur entre les entiers a et b
$\mathrm{csum}(d)$	Somme de contrôle de d

1

Introduction à la cryptographie post-quantique

La cryptographie est au cœur de la sécurisation des infrastructures informatiques, utilisée quotidiennement par des milliards d'utilisateurs. Depuis la fin des années 80, l'hypothèse fondamentale sur laquelle repose la sécurité de la majorité des cryptosystèmes à clé publique déployés en pratique est la difficulté de résoudre deux problèmes mathématiques issus de la théorie des nombres : le calcul du logarithme discret dans un groupe cyclique (problème du logarithme discret, DLOG) et la décomposition de grands entiers en facteurs premiers (problème de la factorisation, FACT).

Les meilleurs algorithmes, utilisant un ordinateur classique, pour résoudre ces problèmes ont des complexités sous-exponentielles, voire exponentielles dans le cas du logarithme discret sur des courbes elliptiques. Pour casser les cryptosystèmes reposant sur ces problèmes, avec les tailles des clés de 2 048 ou 4 096 bits utilisées, il faut un temps de calcul extrêmement long sur un ordinateur classique, dépassant même le nombre d'atomes dans l'univers. Au milieu des années 1990, P. Shor [Sho97] démontre que DLOG et FACT peuvent se résoudre très efficacement, c'est-à-dire en un temps polynomial, sur un ordinateur quantique, rendant ainsi inutiles les primitives cryptographiques basés sur ces problèmes si un tel ordinateur est construit.

La cryptographie *post-quantique*, l'objet de cet ouvrage, s'attache à concevoir de nouveaux cryptosystèmes capables de résister aux ordinateurs quantiques. Ce terme nécessite une précision : nul besoin d'un ordinateur quantique pour faire fonctionner des algorithmes post-quantiques, en effet ils fonctionnent sur les ordinateurs classiques ! Pour preuve, depuis 2025, ces cryptosystèmes sont déployés dans les principaux navigateurs Internet, tels que Chrome ou Firefox, ainsi que dans des applications de messagerie comme celles d'Apple, iMessage, ou de Signal.

Ce premier chapitre présente un panorama des nouveaux problèmes difficiles de la cryptographie post-quantique, ainsi que les principales raisons motivant la migration actuelle vers cette nouvelle cryptographie : les progrès des ordinateurs quantiques, la

perception d'une menace croissante pour les cryptosystèmes actuels avec la possibilité, pas si lointaine, d'un *Q-day* aux conséquences potentiellement catastrophiques, le processus de normalisation post-quantique initié par le NIST, organisme de normalisation américain majeur, ainsi que les feuilles de route établies par de nombreux pays à travers le monde pour achever la migration vers le post-quantique avant 2035.

Q-day

Le jour où l'ordinateur quantique sera en mesure de briser les cryptosystèmes pré-quantiques, c'est-à-dire basés sur DLOG ou FACT, largement utilisés jusqu'à présent, est communément appelé *Q-day*. Un scénario dans lequel ce *Q-day* surviendrait avant le déploiement massif d'une cryptographie résistante au quantique aurait des conséquences catastrophiques. Bien que cette date reste difficile à prévoir avec exactitude, elle est particulièrement scrutée par le monde de la cybersécurité. En 2024, le *Bundesamt für Sicherheit in der Informationstechnik* (BSI), l'agence allemande de sécurité, estime que le *Q-day* pourrait intervenir avant 2040 [Fed24].

1.1 La menace quantique

Lors d'une conférence internationale dédiée à la cryptographie post-quantique en 2014, M. Mariantoni – professeur de physique à l'université de Waterloo au Canada – estimait qu'un ordinateur quantique d'une valeur d'un milliard de dollars pourrait casser le chiffrement Rivest-Shamir-Adelman (RSA) d'ici 2030, en consommant une quantité d'énergie équivalente à celle d'une centrale nucléaire.

L'année suivante, en 2015, l'agence de sécurité américaine, *National Security Agency* (NSA), faisait une autre annonce surprenante. Les progrès des ordinateurs quantiques menacent la sécurité à long terme des normes de cryptographie à clé publique pré-quantique telles que Diffie-Hellman (DH), *Elliptic Curve Diffie-Hellman* (ECDH), *Digital Signature Algorithm* (DSA), *Elliptic Curve Digital Signature Algorithm* (ECDSA), *Edwards-curve DSA* (EdDSA) ou RSA qui sont basées sur les problèmes DLOG ou FACT, dont les définitions sont rappelées ci-dessous.

Problèmes difficiles de la cryptographie pré-quantique

Définition 1.1 (Problème de factorisation)**.** *Étant donné $N = p \cdot q$, avec p, q des entiers premiers, le* problème de factorisation *(FACT) consiste à retrouver p et q à partir de N.*

Définition 1.2 (Problème du logarithme discret)**.** *Soient p un entier, $\mathbb{G}$ un sous-groupe cyclique d'ordre q premier du groupe multiplicatif $\mathbb{Z}_p^\times$ et g un générateur de $\mathbb{G}$. Étant donné $h \equiv g^s \bmod p$ avec $0 \leqslant s < q$, le* problème du logarithme discret *(DLOG) consiste à trouver s, le logarithme discret de h en base g.*

En 2015, ces annonces ont de quoi surprendre puisque la menace posée par l'algorithme de Shor était perçue comme purement théorique. À l'époque, les ordinateurs

quantiques ne disposaient que d'une capacité de calcul très limitée. Depuis, la puissance de ces machines a considérablement augmenté. Le nombre de *qubits* (*quantum bits*, parfois aussi écrit *qbit*) est souvent utilisé comme un indicateur simple pour évaluer les progrès des ordinateurs quantiques. Un qubit est l'équivalent quantique du bit classique, et détermine la taille des problèmes traités par un ordinateur quantique.

L'unique décompte du nombre de qubits s'avère insuffisant pour refléter la puissance réelle des machines quantiques actuelles. D'une part, ces machines se divisent en deux grandes catégories et le nombre de qubits n'a pas la même signification selon le type de machine quantique considéré.

Les calculateurs spécialisés, comme ceux développés par les sociétés D-Wave ou Pasqal, qui exploitent des processeurs quantiques dédiés au *recuit quantique* forment la première catégorie. Ces machines traitent un seul type de problème : l'optimisation de fonctions quadratiques. Par exemple, le problème du voyageur de commerce, qui consiste à déterminer, pour un ensemble de villes, le plus court chemin passant par chaque ville une seule fois, s'écrit comme un problème d'optimisation quadratique. Les applications pratiques sont nombreuses, mais l'impact de ces machines en cryptographie est très limité. L'évolution du nombre de qubits des ordinateurs spécialisés D-Wave est le suivant :

— 2011 : 128 qubits (D-Wave One) ;
— 2013 : 512 qubits (D-Wave Two) ;
— 2015 : 1 152 qubits (D-Wave 2X) ;
— 2017 : 2 048 qubits (D-Wave 2000Q) ;
— 2020 : 5 760 qubits (D-Wave Advantage) ;
— 2024 : 7 440 qubits (D-Wave Advantage2).

La seconde catégorie regroupe les machines quantiques universelles, capables de résoudre tout problème algorithmique. Ce sont ces machines qui permettent notamment d'exécuter les algorithmes de Grover ou Shor, parmi d'autres. L'évolution du nombre de qubits de ces ordinateurs est la suivante :

— 1998 : 2 qubits (*International Business Machines* (IBM)) ;
— 1999 : 3 qubits (IBM) ;
— 2001 : 7 qubits (IBM) ;
— 2017 : 50 qubits (IBM Q50) ;
— 2019 : 53 qubits (Google Sycamore) ;
— 2021 : 90 qubits (Rigetti Aspen-9) ;
— 2021 : 127 qubits (IBM Eagle) ;
— 2023 : 133 qubits (IBM Heron) ;
— 2022 : 433 qubits (IBM Osprey) ;
— décembre 2023 : 1 121 qubits (IBM Condor).

D'autre part, les qubits sont extrêmement sensibles aux perturbations, ce qui entraîne des erreurs et limite leurs performances. Il convient alors de distinguer les qubits *logiques*, qui sont des qubits presque parfaits et auto-corrigés, des qubits *physiques*, qui, eux, sont sujets à des erreurs et possèdent un temps de cohérence limité. Les nombres

de qubits précédents correspondent tous à des qubits physiques. Pour certaines technologies de qubits, l'ordre de grandeur est d'environ 1 000 entre le nombre de qubits physiques et le nombre de qubits logiques.

Suprématie quantique

Le concept de *suprématie quantique* a été introduit par le physicien J. Preskill pour désigner le moment à partir duquel les capacités pratiques de calcul d'un ordinateur quantique surpassera celles des supercalculateurs classiques. En 2019, Google annonçait avoir franchi ce cap avec Sycamore, un processeur quantique universel de 53 qubits physiques [AAB+19]. Les auteurs indiquaient pouvoir résoudre en seulement 200 secondes un problème d'échantillonnage de circuits aléatoires avec ce nouveau processeur quantique. D'après [AAB+19], cette tâche nécessiterait 10 000 ans à l'aide du supercalculateur classique le plus puissant . Cette dernière partie de l'annonce est rapidement remise en cause par la communauté scientifique. De nouvelles techniques algorithmiques permettent maintenant de résoudre le problème considéré par Google en quelques jours, voire en quelques secondes sur des machines classiques.
En 2026, la suprématie quantique n'est donc pas encore une réalité, mais cela n'enlève rien à la prouesse réalisée par Google, qui démontre la faisabilité d'assembler une machine quantique universelle avec un nombre important de qubits. Depuis, Google a construit un processeur quantique universel encore plus puissant, Willow ayant 105 qubits physiques. Par ailleurs, le prix Nobel de physique 2025 a récompensé le Britannique J. Clarke, le Français M. Devoret, et l'Américain J. Martinis pour des travaux fondamentaux sur l'effet tunnel quantique macroscopique ayant ouvert la voie à la réalisation de qubits supraconducteurs, qui sont au cœur de certains prototypes d'ordinateurs quantiques. Le chercheur américain, alors employé par Google, a d'ailleurs contribué à la construction de Sycamore et à l'annonce de la suprématie quantique.

La société IBM est un autre acteur majeur du quantique. Sa feuille de route sur le sujet ⋆ démarre en 2016 avec un processeur de 5 qubits physiques, atteint plus de 1000 qubits physiques en 2023 et ambitionne de construire une machine dépassant 2000 qubits logiques à l'horizon 2033, machine qui serait notamment capable de casser la cryptographie à clé publique pré-quantique déployée en pratique.

L'Union européenne n'est pas en reste dans cette course technologique : elle compte au moins 39 startups qui cherchent à construire un ordinateur quantique, dont Alice & Bob, C12, Pasqal, Quandela, et Quobly pour la France. Le lecteur intéressé par les évolutions du quantique pourra consulter le très complet et détaillé panorama des technologies quantiques publié, chaque année, sur le blog d'O. Ezratty ◇.

La marge de progression reste, heureusement, encore très importante avant qu'un ordinateur quantique ne parvienne à casser les cryptosystèmes basés sur DLOG ou FACT. Plusieurs études se sont penchées sur les ressources nécessaires pour attaquer

⋆. https://www.ibm.com/quantum/technology#roadmap
◇. https://www.oezratty.net/wordpress/

RSA2048 bits, c'est-à-dire factoriser une clé publique RSA de 2048 bits. C'est une taille typique utilisée en pratique avec un niveau de sécurité de 116 bits, la complexité du meilleur algorithme classique nécessite 2^{116} opérations pour factoriser RSA2048. Il faudrait mobiliser des milliers de supercalculateurs pendant plusieurs siècles pour factoriser une telle clé publique.

En 2019, C. Gidney et M. Ekerå [GE21] estimaient qu'environ 20 millions de qubits physiques seraient nécessaires pour casser RSA2048 en 8 heures. L'amélioration de la qualité de qubits ainsi que des nouvelles améliorations de l'algorithme de Shor [CFS25] ont permis de réduire significativement les ressources nécessaires pour effectuer ce calcul. Dans un article de 2025, G. Gidney [Gid25] estime qu'il ne faudrait plus que 1 million de qubits physiques pour RSA2048, qui correspondent à 1399 qubits logiques. En France, le programme PROQCIMA ⋆, porté par le ministère des Armées et France 2030, ambitionne de construire des machines quantiques de 128 qubits logiques d'ici 2032, puis de 2048 qubits logiques d'ici 2035.

Ces résultats montrent que l'incertitude ne porte pas tant sur la capacité à construire une machine quantique de grande capacité, assez puissante pour remettre en cause la cryptographie pré-quantique, que sur le temps nécessaire pour y parvenir.

Le *Q-day* et la menace quantique peuvent cependant sembler lointains. Il est légitime de se demander pourquoi s'en préoccuper. En réalité, le problème se pose déjà pour les communications les plus sensibles, par exemple les secrets à longue durée de vie dont la confidentialité doit être garantie sur plusieurs décennies (secrets d'État ou industriels, données bancaires, biomédicales, etc.).

Capturer maintenant, et déchiffrer plus tard

Cette attaque, « *store now, decrypt later* », consiste à capturer des données chiffrées en attendant qu'un ordinateur quantique suffisamment puissant soit disponible pour en révéler les secrets. Il est possible de collecter massivement des données à grande échelle et de les conserver dans de grands centres de stockage de données. Ensuite, il suffit d'attendre patiemment la mise à disposition d'une machine quantique assez puissante.
Cette technique de cryptanalyse n'est pas vraiment nouvelle et a déjà été utilisée dans le passé. Le projet Venona, par exemple, était un programme mené par les Américains, entre 1943 et 1980, pour casser des messages chiffrés par les Soviétiques, interceptés entre 1940 et 1948. Ces messages ont ensuite été analysés pendant presque 40 ans, avec quelques succès. Si la technique est ancienne, les moyens technologiques actuels permettent de la déployer à une échelle planétaire, comme l'a révélé E. Snowden.

Les objets connectés à longue durée de vie, comme les voitures connectées, les avions ou les satellites, sont également concernés. Déployés pendant plusieurs décennies, la mise à jour des composants cryptographiques est très complexe, voire impossible.

⋆. https://quantique.france2030.gouv.fr/acces-aux-marches/programme-proqcima/