CRYSTALS-Kyber ML-KEM : Cryptographie Post-Quantique NIST

Points essentiels

- ML-KEM (FIPS 203) standardise CRYSTALS-Kyber depuis août 2024 au NIST
- Kyber repose sur Module-LWE, résistant à l'algorithme de Shor
- Trois variantes : Kyber-512, Kyber-768 recommandé, Kyber-1024 pour usages gouvernementaux
- L'ANSSI impose l'inventaire cryptographique et la migration hybride des infrastructures PKI

À RETENIR

À retenir

ML-KEM (FIPS 203) standardise CRYSTALS-Kyber depuis août 2024 au NIST

Kyber repose sur Module-LWE, résistant à l'algorithme de Shor

Trois variantes : Kyber-512, Kyber-768 recommandé, Kyber-1024 pour usages gouvernementaux

L'ANSSI impose l'inventaire cryptographique et la migration hybride des infrastructures PKI

La menace quantique n'est plus une hypothèse académique confinée aux laboratoires : elle figure désormais dans les feuilles de route réglementaires françaises et européennes, dans les avis de l'ANSSI et dans les exigences de sécurité des marchés publics. CRYSTALS-Kyber, standardisé sous l'identifiant ML-KEM (FIPS 203), constitue aujourd'hui le mécanisme d'encapsulation de clés de référence pour résister aux futurs calculateurs quantiques. Retenu à l'issue d'un processus de sélection long de huit ans, CRYSTALS-Kyber post-quantique NIST s'appuie sur la difficulté

du problème Module-LWE sur les réseaux euclidiens, une base mathématique qu'aucun algorithme quantique connu ne sait casser efficacement. Cet article détaille son fonctionnement cryptographique, ses trois niveaux de sécurité, ses performances comparées à RSA et ECDH, ainsi que les étapes concrètes d'une migration hybride vers la cryptographie post-quantique en entreprise.

À RETENIR

⚡ À retenir — CRYSTALS-Kyber / ML-KEM

ML-KEM (ex-Kyber) est le standard NIST FIPS 203 pour l'encapsulation de clé post-quantique. Il existe en trois variantes : Kyber-512 (sécurité 128 bits), Kyber-768 (192 bits, recommandée pour la plupart des usages professionnels) et Kyber-1024 (256 bits, usage gouvernemental et défense). Les RSSI français doivent initier leur inventaire cryptographique dès maintenant et cibler une migration complète des systèmes critiques d'ici 2028-2030, conformément aux recommandations ANSSI.

La menace quantique : chronologie et réalité pour les DSI françaises

L'ordinateur quantique cryptographiquement pertinent (CRQC — Cryptographically Relevant Quantum Computer) est un système capable d'exécuter l'algorithme de Shor à une échelle suffisante pour factoriser des clés RSA-2048 en un temps raisonnable. Les estimations actuelles des experts convergent vers une fenêtre de 2030-2035 pour les premières démonstrations opérationnelles, et 2035-2040 pour un déploiement à grande échelle. Cette timeline peut sembler lointaine, mais elle ne l'est pas du point de vue de la sécurité de l'information pour trois raisons majeures.

> En pratique, les incidents que nous traitons révèlent que l'écart entre politiques de sécurité documentées et application réelle est presque toujours plus grand que prévu. La vérification terrain régulière reste la seule façon de mesurer ce delta.

> *— Retour terrain, Ayi NEDJIMI Consultants*

Première raison : la durée de vie des données sensibles. Des informations classifiées chiffrées aujourd'hui avec RSA-4096 seront potentiellement déchiffrables dans 10 à 15 ans par un acteur disposant d'un CRQC. Les attaques de type *harvest now, decrypt later* (collecter maintenant, déchiffrer plus tard) sont déjà documentées et pratiquées par des services de renseignement étatiques : des flux TLS sont capturés et stockés en vue d'un déchiffrement futur. Pour toute organisation traitant des données à valeur stratégique sur le long terme — propriété intellectuelle industrielle, données médicales, secrets de fabrication, communications diplomatiques —, la fenêtre de vulnérabilité effective est déjà ouverte.

Deuxième raison : les cycles de remplacement des infrastructures. Migrer une infrastructure PKI d'entreprise, un HSM gouvernemental, un système embarqué industriel ou une carte à puce prend typiquement 3 à 7 ans entre la décision et le déploiement complet. Les cycles d'achat des équipements critiques (pare-feux, VPN concentrateurs, HSM) impliquent que les systèmes achetés aujourd'hui seront encore en production en 2032-2035. Si ces systèmes ne supportent pas ML-KEM nativement, leur remplacement prématuré générera des coûts considérables.

Troisième raison : les contraintes réglementaires. L'ANSSI a publié ses premières recommandations sur la migration post-quantique et a annoncé une révision du Référentiel Général de Sécurité (RGS v3) intégrant des exigences post-quantiques. Les appels d'offres de la DGA et des ministères régaliens commencent à intégrer des clauses de *crypto-agilité* comme critère d'évaluation. Pour les entités soumises à NIS 2 et au ReCyF ANSSI, la cryptographie post-quantique s'inscrit dans la mesure 5 (sécurité des communications) et la mesure 8 (cryptographie et chiffrement).

CRYSTALS-Kyber : origine, conception et fondements mathématiques

CRYSTALS-Kyber est né du projet **CRYSTALS** (*Cryptographic Suite for Algebraic Lattices*), une initiative de recherche collaborative impliquant IBM Research, CWI Amsterdam, Ruhr-Universität Bochum, et plusieurs autres institutions. Soumis au processus de standardisation du NIST en 2017 lors de l'appel à candidatures Post-Quantum Cryptography, Kyber a traversé les

rounds de sélection 1 (2019), 2 (2020) et 3 (2021) pour être retenu comme finaliste unique dans la catégorie *Key Encapsulation Mechanism* (KEM). La standardisation finale a été publiée en août 2024 sous le nom **ML-KEM, FIPS 203**.

Le fondement mathématique de Kyber repose sur le problème **Module Learning With Errors (MLWE)**, une variante modulaire du problème LWE introduit par Oded Regev en 2005. Le problème LWE peut être défini ainsi : étant donné un vecteur aléatoire *s* (le secret), un ensemble de paires (a_i, b_i) où b_i = ⟨a_i, s⟩ + e_i avec e_i un bruit gaussien discret de petite amplitude, retrouver *s* est computationnellement difficile, même pour un ordinateur quantique. MLWE généralise ce problème à des matrices de polynômes sur des anneaux quotients, ce qui permet d'obtenir des performances nettement supérieures à LWE simple tout en maintenant des garanties de sécurité prouvables sous des hypothèses standard.

Concrètement, Kyber utilise un anneau de polynômes R_q = Z_q[X]/(X^n + 1) avec n=256 et q=3329. La clé publique est une matrice A ∈ R_q^{k×k} tirée de manière pseudo-aléatoire (via SHAKE-128) et un vecteur b = As + e, où s et e sont des vecteurs à coefficients petits. L'encapsulation génère un secret partagé et un chiffré (ciphertext) ; la décapsulation retrouve le secret partagé à partir du chiffré et de la clé privée. La sécurité est réduite à la difficulté de MLWE, pour laquelle les meilleurs algorithmes quantiques connus — y compris les variantes de l'algorithme de Grover — n'offrent pas d'avantage exploitable à l'échelle pratique.

Standardisation NIST 2024 : FIPS 203, 204 et 205

La publication du NIST en août 2024 a introduit trois standards post-quantiques complémentaires qui constituent le socle de la cryptographie post-quantique pour les prochaines décennies :

FIPS 203 — ML-KEM (ex-Kyber) : mécanisme d'encapsulation de clé pour l'établissement de clés dans les protocoles de type TLS, SSH, VPN, messagerie chiffrée. Remplace ECDH et RSA-KEM.

FIPS 204 — ML-DSA (ex-Dilithium) : algorithme de signature numérique basé sur les réseaux euclidiens. Remplace RSA-PSS et ECDSA pour la signature de certificats, de firmwares, de logiciels et de documents.

FIPS 205 — SLH-DSA (ex-SPHINCS+) : algorithme de signature basé sur les fonctions de hachage, offrant une sécurité conservative (pas de problème algébrique structuré susceptible de nouvelles attaques). Complémentaire de ML-DSA pour les cas d'usage haute assurance.

Un quatrième standard, **FIPS 206 — FN-DSA (ex-FALCON)**, a été ajouté par le NIST en 2024 : il offre des signatures plus compactes que ML-DSA au prix d'une implémentation plus complexe, particulièrement adapté aux environnements contraints (IoT, cartes à puce). Pour les RSSI, la compréhension de l'écosystème complet est importante : ML-KEM gère l'échange de clés, ML-DSA ou FN-DSA gèrent la signature — les deux sont nécessaires pour sécuriser une infrastructure PKI complète. Les ressources techniques officielles sont disponibles sur le site NIST PQC.

Les trois variantes de Kyber : choisir le bon niveau de sécurité

ML-KEM est disponible en trois variantes paramétriques, correspondant à des niveaux de sécurité NIST différents :

ML-KEM-512 (Kyber-512) : niveau de sécurité NIST 1, équivalent à AES-128. Taille de clé publique 800 octets, taille de chiffré 768 octets. Adapté aux environnements très contraints (IoT, cartes à puce, protocoles haute fréquence). Non recommandé pour les applications gouvernementales ou de défense.

ML-KEM-768 (Kyber-768) : niveau de sécurité NIST 3, équivalent à AES-192. Taille de clé publique 1184 octets, taille de chiffré 1088 octets. **La variante recommandée pour la grande majorité des applications professionnelles** : messagerie d'entreprise, VPN, TLS 1.3, stockage chiffré. Offre un excellent compromis performance/sécurité.

ML-KEM-1024 (Kyber-1024) : niveau de sécurité NIST 5, équivalent à AES-256. Taille de clé publique 1568 octets, taille de chiffré 1568 octets. Recommandé pour les applications

gouvernementales, de défense, de renseignement, et pour les données à durée de vie sensible supérieure à 20 ans.

Par comparaison, une clé publique RSA-2048 fait 256 octets, et ECDH P-256 utilise des clés de 64 octets. Le surcoût en taille de Kyber est réel mais gérable dans la plupart des contextes : pour TLS 1.3, le ClientHello augmente de moins de 2 Ko, ce qui est négligeable sur les connexions modernes. En revanche, les environnements à très forte contrainte de bande passante (protocoles embarqués, satellite à faible débit, réseaux LoRaWAN) nécessitent une évaluation spécifique.

Intégration pratique : TLS 1.3, OpenSSL, Go et les grands acteurs

L'adoption de ML-KEM dans les stacks cryptographiques majeures est déjà en cours. Voici un panorama des intégrations disponibles en production ou en déploiement avancé en 2026 :

TLS 1.3 hybride (X25519Kyber768) : l'IETF a standardisé un mode hybride combinant ECDH X25519 et Kyber-768 pour l'échange de clés TLS, identifié par le code de groupe 0x6399. Ce mode hybride est la stratégie recommandée pour la période de transition : il maintient la sécurité classique (X25519) tout en ajoutant la protection post-quantique (Kyber-768). Google Chrome a activé ce mode en 2023 pour une large fraction de ses connexions HTTPS ; Cloudflare le déploie sur ses edge nodes depuis 2024. La spécification IETF est disponible dans le draft IETF TLS Hybrid Design.

OpenSSL 3.x : depuis OpenSSL 3.2, ML-KEM-768 est disponible via le provider OQS (Open Quantum Safe). En 2026, l'intégration native dans le provider standard d'OpenSSL est en cours de finalisation. Les distributions Linux majeures (Debian, Ubuntu, RHEL) commencent à livrer OpenSSL avec le support OQS en option.

Go 1.23+ : le package standard `crypto/mlkem` a été ajouté dans Go 1.23, permettant une intégration native de ML-KEM-768 et ML-KEM-1024 sans dépendances tierces. Les équipes DevSecOps travaillant sur des infrastructures Windows sécurisées peuvent intégrer Kyber dans leurs outils Go existants sans complexité supplémentaire.

Bouncy Castle (Java/.NET) : les bibliothèques Bouncy Castle supportent ML-KEM depuis la version 1.78 (Java) et 2.3 (.NET). C'est le chemin recommandé pour les applications Java/Spring Boot et .NET/ASP.NET qui ne peuvent pas encore s'appuyer sur la JVM ou le CLR standard.

AWS, Azure, GCP : les trois hyperscalers ont annoncé des plans de support ML-KEM dans leurs services cryptographiques managés (KMS, HSM cloud) pour 2025-2026. AWS KMS supporte déjà ML-KEM en préversion pour certaines régions.

Impact pour les RSSI : inventaire cryptographique et crypto-agilité

La migration vers ML-KEM n'est pas un simple remplacement de bibliothèque : c'est un projet de transformation de l'infrastructure cryptographique qui nécessite une approche méthodique. La première étape, souvent sous-estimée, est l'**inventaire cryptographique** : identifier l'ensemble des systèmes, applications, protocoles et équipements qui utilisent de la cryptographie asymétrique classique (RSA, ECDH, ECDSA, DH).

Cet inventaire révèle systématiquement des angles morts : des certificats générés par des scripts oubliés, des VPN dont le firmware n'est plus maintenu, des APIs legacy utilisant RSA-1024, des HSM dont le contrat de support a expiré. Sans inventaire exhaustif, toute stratégie de migration post-quantique est fragile. La checklist sécurité Active Directory inclut des contrôles sur l'utilisation de protocoles cryptographiques, point de départ utile pour l'inventaire dans les environnements Windows.

Le concept de **crypto-agilité** est central dans cette démarche : il désigne la capacité d'un système à changer d'algorithme cryptographique sans refonte architecturale majeure. Les systèmes crypto-agiles abstraient l'algorithme cryptographique derrière une interface paramétrable (un identifiant d'algorithme dans la configuration, non dans le code) et peuvent basculer de RSA à ML-KEM ou de AES-128 à AES-256 par simple modification de configuration. Les architectures monolithiques où l'algorithme est codé en dur sont les plus vulnérables et les plus coûteuses à migrer.

Pour évaluer le niveau de maturité en crypto-agilité et les obligations réglementaires associées à la migration post-quantique, le benchmark des outils IA de cybersécurité présente plusieurs

solutions d'analyse et de détection de configurations cryptographiques faibles automatisables en SOAR ou XDR. Les exigences de conformité NIS 2 relatives à la cryptographie — mesure 8 du ReCyF ANSSI — sont détaillées dans notre mapping ReCyF ANSSI vs NIS 2.

Vulnérabilités et points d'attention sur ML-KEM

ML-KEM est un algorithme solide, mais son déploiement pratique comporte des risques qu'un RSSI doit connaître. Les vulnérabilités documentées ne remettent pas en cause la solidité mathématique de Kyber, mais concernent ses **implémentations**.

Attaques par canal auxiliaire (side-channel) : comme tout algorithme cryptographique, Kyber peut être vulnérable aux attaques par canal auxiliaire (timing, consommation électrique, rayonnement électromagnétique) si l'implémentation n'est pas soigneusement durcie. Des travaux académiques ont démontré des attaques timing sur des implémentations non-constant-time de Kyber. Les implémentations de référence (liboqs, Go crypto/mlkem) sont conçues pour être constant-time, mais des portages maison peuvent réintroduire ces vulnérabilités.

Génération de nombres aléatoires : la sécurité de Kyber dépend de la qualité du générateur de nombres pseudo-aléatoires (PRNG) utilisé pour générer les clés et les termes de bruit. Un PRNG faible ou mal initialisé peut compromettre complètement la sécurité, indépendamment de la solidité mathématique de l'algorithme. Cette contrainte s'applique à toutes les implémentations : utiliser uniquement des sources d'entropie de haute qualité (getrandom() sous Linux, BCryptGenRandom sous Windows, HSM hardware).

Mode hybride obligatoire durant la transition : jusqu'à ce que la résistance de ML-KEM aux attaques classiques soit définitivement validée par la communauté cryptographique sur la durée, les autorités (NIST, ANSSI, ENISA) recommandent de déployer ML-KEM en mode hybride avec un algorithme classique éprouvé (X25519 + ML-KEM-768 pour TLS). Cette recommandation vaut pour au moins la période 2024-2028.

Gestion des clés post-quantiques : les clés ML-KEM sont plus volumineuses que les clés ECDH. Les systèmes de gestion de clés (KMS, HSM) doivent être vérifiés pour leur capacité à stocker, distribuer et révoquer des clés de cette taille. En particulier, les annuaires LDAP/Active

Directory contenant des certificats devront être vérifiés pour les limites de taille d'attribut. Les pratiques de gestion de certificats documentées dans notre guide DMARC/DKIM/SPF (rotation de clés, révocation) s'appliquent également aux clés ML-KEM.

Comparaison : ML-KEM face aux autres finalistes NIST PQC

ML-KEM n'est pas le seul algorithme post-quantique candidat. Comprendre ses avantages et limites par rapport aux alternatives aide à choisir la bonne solution pour chaque cas d'usage :

ML-KEM (Kyber) : lattice-based, excellentes performances, petites tailles de clé comparées aux autres finalists, large adoption industrielle, support NIST officiel. Recommandé pour la grande majorité des usages.

BIKE et HQC : code-based (théorie des codes correcteurs d'erreurs). Alternatives de diversité algorithmique recommandées par le NIST pour les cas où une seconde option est nécessaire. Tailles de clé plus grandes (plusieurs Ko). BIKE et HQC sont en phase de standardisation NIST (round 4).

Classic McEliece : code-based, extrêmement conservateur et éprouvé depuis 1978. Clés publiques très volumineuses (261 Ko pour McEliece-6960119), ce qui le rend impraticable pour la plupart des protocoles réseau. Adapté aux HSM offline et aux applications à très long terme.

NTRU : lattice-based, ancêtre de Kyber, moins performant et retiré du processus NIST round 4 par ses auteurs. Non recommandé pour les nouveaux déploiements.

FrodoKEM : LWE-based (non modulaire), plus conservateur que Kyber mais moins performant. Alternative sérieuse pour les applications gouvernementales haute assurance qui souhaitent éviter toute structure algébrique modulaire.

Le consensus de la communauté cryptographique est clair : ML-KEM (Kyber) est le premier choix pour les KEM post-quantiques dans la quasi-totalité des contextes. Les alternatives ont leur place dans des architectures de diversité algorithmique — certains systèmes gouvernementaux déploient ML-KEM + BIKE en parallèle pour se protéger contre d'éventuelles faiblesses découvertes dans l'un ou l'autre.

Plan de migration post-quantique pour une DSI française (2025–2030)

Voici les étapes d'une migration structurée, adaptée aux contraintes des organisations françaises soumises à NIS 2 et aux recommandations ANSSI :

Phase 1 — Inventaire et priorisation (2025-2026) : réaliser un inventaire exhaustif de tous les actifs cryptographiques (certificats, clés, protocoles, équipements). Classer les actifs par criticité et durée de vie des données protégées. Identifier les systèmes non-crypto-agiles nécessitant une refonte architecturale. Évaluer les fournisseurs et prestataires sur leur roadmap post-quantique. Cette phase produit une cartographie cryptographique qui sera le document de référence pour toute la migration.

Phase 2 — Mise à jour des composants (2026-2027) : mettre à jour les bibliothèques cryptographiques (OpenSSL, JDK, .NET) vers des versions supportant ML-KEM. Activer le mode hybride TLS 1.3 (X25519Kyber768) sur tous les reverse proxies, load balancers et API gateways. Mettre à jour ou remplacer les HSM dont le firmware ne supporte pas ML-KEM. Commencer la migration des PKI internes vers des CA supportant ML-DSA.

Phase 3 — Migration des applications critiques (2027-2028) : migrer les applications à données sensibles à long terme vers ML-KEM natif (sans hybride). Mettre à jour les protocoles internes (messagerie interne, protocoles OT/ICS, authentification forte). Révoquer les anciens certificats RSA/ECDSA et les remplacer par des certificats ML-DSA. Réaliser des audits de conformité post-quantique.

Phase 4 — Consolidation et conformité (2028-2030) : désactiver progressivement les algorithmes classiques (RSA, ECDH) sur les systèmes internes. Mettre à jour les politiques de sécurité, les documents PSSI et les analyses de risques. Démontrer la conformité post-quantique lors des audits ANSSI (NIS 2, RGS v3). Former et certifier les équipes techniques sur la cryptographie post-quantique.

FAQ — CRYSTALS-Kyber et la cryptographie post-quantique

Kyber est-il vraiment sûr contre les ordinateurs quantiques actuels ?

Oui. La sécurité de ML-KEM repose sur le problème MLWE, pour lequel il n'existe pas d'algorithme quantique efficace connu — ni parmi les algorithmes déjà publiés, ni parmi ceux en développement dans les laboratoires de recherche. Les meilleurs algorithmes quantiques connus (variantes de l'algorithme de Grover) n'offrent qu'une accélération quadratique contre MLWE, ce qui est compensé par les tailles de paramètre de Kyber. Cela dit, la communauté cryptographique continue de surveiller activement la recherche, et le mode hybride (X25519 + Kyber) est recommandé pendant la période de transition pour conserver la protection classique en cas de découverte inattendue.

Quelle variante de Kyber choisir pour une entreprise française soumise à NIS 2 ?

Pour la grande majorité des cas d'usage professionnels — TLS 1.3, VPN d'entreprise, messagerie sécurisée, authentification — **ML-KEM-768** est la variante recommandée. Elle offre un niveau de sécurité NIST 3 (équivalent AES-192), des performances excellentes sur les CPU modernes, et des tailles de clé compatibles avec tous les protocoles réseau standards. ML-KEM-1024 est réservé aux applications gouvernementales, de défense, et aux données dont la durée de vie sensible dépasse 20 ans. ML-KEM-512 peut être envisagé pour les environnements IoT très contraints, à condition que le niveau de sensibilité des données le justifie.

Combien de temps faut-il pour migrer une infrastructure PKI vers ML-KEM ?

La durée dépend fortement de la complexité et de la taille de l'infrastructure. Pour une PME avec une PKI simple (une CA interne, quelques centaines de certificats), la migration technique peut prendre 3 à 6 mois. Pour une grande entreprise ou une administration avec plusieurs CA hiérarchiques, des milliers de certificats, des équipements hétérogènes et des contraintes de disponibilité élevées, le projet dure typiquement 2 à 4 ans. L'inventaire cryptographique est l'étape qui prend le plus de temps (40 à 60% du projet) car elle révèle systématiquement des

actifs inattendus. Commencer maintenant est la recommandation universelle des experts et des autorités régulatrices.

Quand l'ANSSI imposera-t-elle ML-KEM dans le RGS ?

L'ANSSI n'a pas encore publié de date officielle pour l'intégration de ML-KEM dans le RGS v3, mais les signaux sont clairs : des recommandations préliminaires sur la migration post-quantique ont été publiées, et les marchés publics de défense et de renseignement commencent à intégrer des critères post-quantiques dans leurs cahiers des charges. L'horizon le plus probable pour une obligation réglementaire formelle dans le RGS est 2027-2028, ce qui laisse une fenêtre de 2 à 3 ans pour les organisations qui n'ont pas encore initié leur migration — mais cette fenêtre se réduit rapidement si l'on tient compte des délais de projet.

Variante ML-KEM	Niveau de sécurité NIST	Clé publique / Chiffré (octets)	Équivalent symétrique	Usage recommandé
ML-KEM-512 (Kyber-512)	Catégorie 1	800 / 768	AES-128	IoT, environnements contraints, données à faible durée de vie
ML-KEM-768 (Kyber-768)	Catégorie 3	1 184 / 1 088	AES-192	Choix par défaut : TLS 1.3, VPN, messagerie chiffrée
ML-KEM-1024 (Kyber-1024)	Catégorie 5	1 568 / 1 568	AES-256	Secret Défense, OIV/OSE, données à longévité > 20 ans
X25519MLKEM768 (hybride)	Catégorie 3 + classique	1 216 / 1 120	AES-192	Mode exigé par l'ANSSI en phase de transition (défense en profondeur)
RSA-2048 (référence)	Aucune (cassé par Shor)	256 / 256	≈ AES-112	À inventorier puis remplacer : vulnérable au « harvest now, decrypt later »
ECDH P-256 (référence)	Aucune (cassé par Shor)	64 / 64	≈ AES-128	À conserver uniquement en composante hybride, jamais seul
ML-DSA / FIPS 204 (complément)	Catégories 2 à 5	1 312 / 2 420 (signature)	AES-128 à AES-256	Signature PKI et code signing, à coupler avec ML-KEM

Conclusion

Ce sujet s'inscrit dans un contexte de menaces en constante évolution. La meilleure protection combine veille active, audits réguliers et sécurité by design. Pour approfondir ou évaluer votre exposition, consultez nos experts.

>