Historia Y Desarrollo De La Encriptación Post Cuántica Con Ia: Revisión

History And Development Of Post-Quantum Encryption Using Ai: A Review

PhD. J. P. Muñoz-Toriz [a]
Mcs. Jessica M. Cucaita-Castro [b]
PhD. L. D. Lara-Rodríguez [c]
PhD. E. López-Meléndez [d]

[a] Academia de Matemáticas, Unidad Profesional Interdisciplinaria de Ingeniería Campus Tlaxcala, Instituto Politécnico Nacional, Tlaxcala, México.
jpmunozt@ipn.mx . ORCID: 0000-0002-2281-2224
[b] Programa de Ciencia de Datos. Universidad Tecnológica Latinoamericana en Línea, Naucalpan de Juárez, México.jessicmcucaita@gmail.com ORCID: 0009-0006-5768-6850
[c] Facultad de Mecatrónica, Biónica y Aeroespacial, Universidad Popular Autónoma del Estado de Puebla, Puebla, México. luisdavid.lara@upaep.mx ORCID: 0000-0001-9700-390X
[d] División de Mecatrónica, Universidad Tecnológica de Huejotzingo, Huejotzingo, México.
elizabeth.lopez@uth.edu.mx ORCID: 0000-0002-1241-3289

Resumen

La criptografía post cuántica (PQC) ha transitado en menos de una década de tema teórico a problema urgente de ingeniería de sistemas. La publicación en agosto de 2024 de los estándares FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA) por parte del NIST inauguró una fase de despliegue activo, mientras que la inteligencia artificial (IA) emergió como habilitador transversal del proceso. Este artículo presenta una revisión narrativa estructurada del estado del arte en la intersección entre IA, PQC y migración quantum-safe, organizada en torno a seis ejes temáticos: fundamentos PQC, optimización de implementaciones asistida por IA, ataques de canal lateral con aprendizaje profundo sobre PQC, orquestación automatizada de la migración, IA como vector de ataque emergente y brechas metodológicas. La búsqueda bibliográfica abarcó cinco bases de datos académicas entre 2019 y 2026. Los hallazgos identifican brechas críticas en evaluación formal frente a adversarios de aprendizaje profundo, ausencia de datasets estándar reproducibles para SCA-DL sobre PQC e integración limitada en entornos restringidos del Internet de las Cosas. Se concluye que la consolidación de marcos de cripto-agilidad asistidos por IA constituye la frontera prioritaria para la próxima fase de la migración global.

Palabras clave: criptografía poscuántica, inteligencia artificial, ataques de canal lateral, migración quantum-safe, cripto-agilidad.

Abstrac

Post-quantum cryptography (PQC) has shifted in less than a decade from a theoretical research topic to an urgent systems engineering problem. The publication of NIST standards FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) in August 2024 inaugurated an active deployment phase, while artificial intelligence (AI) emerged as a transversal enabler of the migration process. This article presents a structured narrative review of the state of the art at the intersection of AI, PQC, and quantum-safe migration, organized around six thematic axes: PQC foundations, AI-assisted implementation optimization, deep-learning side-channel attacks on PQC, automated orchestration of migration, AI as an emerging attack vector, and methodological gaps. The bibliographic search covered five academic databases between 2019 and 2026. Findings identify critical gaps regarding formal evaluation against deep-learning adversaries, the absence of reproducible standard datasets for DL-SCA on PQC, and limited integration in resource-constrained Internet of Things environments. We conclude that the consolidation of AI-enabled cryptographic agility frameworks is the priority frontier for the next phase of global migration.

Keywords: post-quantum cryptography, artificial intelligence, side-channel attacks, quantum-safe migration, cryptographic agility.

Introducción

La protección matemática de las comunicaciones acompaña a la humanidad desde la Antigüedad, pero ha experimentado durante el último siglo una aceleración sin precedentes que culminó en agosto de 2024 con la publicación de los primeros tres estándares federales de criptografía post cuántica (PQC) por parte del Instituto Nacional de Estándares y Tecnología (NIST). La presente revisión sitúa la transición actual hacia la PQC en el contexto de su trayectoria histórica y examina el papel transversal de la inteligencia artificial (IA), tanto como amenaza emergente como habilitador de la migración hacia infraestructuras quantum-safe. Antes de abordar el estado del arte, conviene resumir los antecedentes que conducen al problema actual.

1.1. Antecedentes históricos: de la criptografía clásica al desafío post cuántico

La criptografía clásica se organizó tradicionalmente en torno a dos primitivas: la transposición y la sustitución. La escítala lacedemonia, mencionada en fuentes griegas del siglo V a. C., consistía en una cinta enrollada alrededor de un bastón cuyo diámetro constituía la clave; el receptor, en posesión de un bastón idéntico, podía recuperar el mensaje al volver a enrollar la cinta. El cifrado de César, atribuido a Julio César y empleado con fines militares hacia el siglo I a. C., aplicaba una sustitución monoalfabética definida por la transformación $C=M+3 \bmod 26$, donde cada letra del mensaje se desplazaba un número fijo de posiciones (Dooley, 2013; Fernández, 2004). Estos sistemas mantuvieron su vigencia durante más de un milenio.

En el siglo IX, el matemático árabe Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi describió el análisis de frecuencias, técnica que rompía sistemáticamente cualquier cifrado monoalfabético al comparar la distribución de símbolos del texto cifrado con la distribución conocida del idioma original. Este avance forzó la aparición de los cifrados polialfabéticos, sistematizados en el siglo XVI por Blaise de Vigenère, que empleaban múltiples alfabetos para diluir las regularidades estadísticas del texto plano. La Primera Guerra Mundial impulsó significativamente el desarrollo de las telecomunicaciones cifradas, transformando tanto el comercio como las estrategias militares (Dooley, 2024).

La era mecánica alcanzó su culminación con la máquina Enigma, desarrollada hacia 1923 por Hugo A. Koch y Arthur Scherbius para cifrar comunicaciones bancarias e industriales y posteriormente adoptada por las fuerzas armadas alemanas durante la Segunda Guerra Mundial. Enigma operaba mediante involuciones permutaciones de orden dos sobre un alfabeto de 26 caracteres, lo que hacía coincidir los procesos de cifrado y descifrado. En 1940, el equipo dirigido por Alan Turing en Bletchley Park desarrolló la Bomba (también conocida como Ultra), capaz de descifrar 84.000 mensajes Enigma al mes hacia 1943. La posterior aparición de la máquina alemana Tunny y la creación de Coloso el primer ordenador electrónico a gran escala y del diseño Automatic Computing Engine (ACE) en 1945 establecieron las bases de la informática moderna (Copeland, 2012; Hoffstein et al., 2014).

La criptografía moderna emerge a partir de tres acontecimientos sucesivos. Primero, la publicación en 1948 de la Teoría Matemática de la Comunicación de Claude Shannon, que cuantificó por primera vez el contenido informacional de un mensaje y estableció los criterios de difusión y confusión que guían el diseño de cifrados desde entonces. Segundo, la estandarización en 1974 del Data Encryption Standard (DES), creado por Horst Feistel y adoptado como primer cifrado simétrico de aceptación pública, que operaba sobre bloques de 64 bits con clave efectiva de 56 bits. Tercero, el trabajo seminal de Whitfield Diffie y Martin Hellman en 1976 sobre el cifrado de clave pública, que introdujo la criptografía asimétrica y abrió la puerta al sistema RSA propuesto por Rivest, Shamir y Adleman en 1977 basado en la dificultad de factorización de enteros grandes y posteriormente a la criptografía de curva elíptica (ECC) propuesta independientemente por Koblitz y Miller en 1985, que ofrece seguridad equivalente con claves significativamente menores (Al-Shabi, 2019; Centellas Claros et al., 2022; Pousa et al., 2011).

Esta arquitectura asimétrica clásica RSA, Diffie-Hellman, ECC sustenta hoy los protocolos TLS, IPsec, SSH, las firmas digitales y la mayoría de los sistemas de identidad digital del mundo. Su seguridad depende, sin embargo, de la dificultad computacional de la factorización entera y del logaritmo discreto, dos problemas que un computador cuántico criptoanalíticamente relevante podría resolver en tiempo polinomial mediante el algoritmo de Shor (1994). El anuncio en 2019 del procesador Sycamore de Google, que resolvió en 200 segundos un problema estimado en 10.000 años para la supercomputadora clásica más avanzada del momento, evidenció que la maduración del hardware cuántico ya no es una hipótesis teórica remota sino una trayectoria tecnológica activa (Arute et al., 2019; Sharbaf, 2011). Es

precisamente esta transición la que convierte a la criptografía post cuántica en un problema urgente de ingeniería de sistemas.

En respuesta a esta amenaza, el NIST lanzó en 2016 un proceso competitivo de estandarización que culminó en agosto de 2024 con la publicación simultánea de tres estándares federales: FIPS 203 (ML-KEM, basado en CRYSTALS-Kyber), FIPS 204 (ML-DSA, basado en CRYSTALS-Dilithium) y FIPS 205 (SLH-DSA, basado en SPHINCS+)(Alagic et al., 2025; Radanliev et al., 2026). A estos se suman el borrador FIPS 206 (FN-DSA, basado en Falcon) y la selección continua de HQC como alternativa de encapsulamiento basada en códigos.

Paralelamente, la inteligencia artificial (IA) y, en particular, el aprendizaje profundo (deep learning, DL) se han consolidado como tecnologías habilitadoras transversales en el ecosistema criptográfico. Su impacto se manifiesta en cuatro frentes: la optimización de parámetros y aceleración de implementaciones PQC en hardware embebido (Sobuj et al., 2026; Yi, 2023); la potenciación de ataques de canal lateral, donde modelos neuronales han demostrado recuperar claves secretas con un número drásticamente reducido de trazas (Marzougui et al., 2022; Ravi et al., 2024); el descubrimiento y priorización automatizada de activos criptográficos vulnerables a escala empresarial, central en marcos de cripto-agilidad (Shaw, 2026; Zhang, 2026); y la detección adaptativa de anomalías en tráfico cifrado en entornos del Internet de las Cosas (Chaganti, 2025; Saeed, 2025).

Esta convergencia entre PQC e IA, sin embargo, presenta una literatura fragmentada. Existen revisiones consolidadas sobre PQC en sí misma (Choudhury et al., 2025; Sakwa & Li, 2026) y revisiones independientes sobre IA en criptografía clásica (Nitaj & Rachidi, 2023; Zolfaghari & Koshiba, 2022), pero la intersección "IA como habilitador y amenaza simultánea de la migración quantum-safe" carece de una síntesis sistemática que articule todos sus planos: matemático, de implementación, de evaluación de seguridad y de orquestación a escala (Chang & Khan, 2026; Saeed, 2025) .

El objetivo de la presente revisión consiste en mapear, estructurar y analizar críticamente el estado del arte en la intersección entre IA, PQC y migración quantum-safe, identificando brechas metodológicas y líneas futuras de investigación pertinentes para la comunidad científica latinoamericana e internacional.

La pregunta de investigación que guía la revisión es: ¿qué técnicas de IA se han aplicado a qué desafíos del ciclo de vida PQC, con qué resultados verificables, y qué brechas persisten para una adopción industrial robusta? El artículo se estructura en siete secciones tras esta introducción: la sección 2 expone la metodología; la sección 3 sintetiza los fundamentos PQC y los estándares vigentes; la sección 4 examina

la IA aplicada a la optimización e implementación eficiente de algoritmos PQC; la sección 5, la más extensa por concentrar la mayor producción reciente, analiza los ataques de canal lateral asistidos por IA y sus contramedidas; la sección 6 aborda la IA en la orquestación de la migración; la sección 7 discute la IA como vector de ataque emergente; y la sección 8 sintetiza brechas de investigación y líneas futuras antes de las conclusiones.

Metodología

La presente revisión adoptó un enfoque narrativo estructurado orientado a sintetizar el estado del arte en la intersección entre inteligencia artificial y criptografía post cuántica, incluyendo los procesos de migración hacia infraestructuras quantum-safe. La búsqueda bibliográfica se realizó entre enero de 2019 y mayo de 2026 en cinco bases de datos académicas: IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink y Google Scholar; se consultaron adicionalmente los repositorios arXiv y SSRN para capturar trabajos recientes en proceso de publicación arbitrada. Las cadenas de búsqueda combinaron términos en inglés relativos a los ejes temáticos de la revisión, incluyendo: post-quantum cryptography, lattice-based cryptography, machine learning, deep learning, side-channel attack, quantum-safe migration, cryptographic agility e IoT security. Se priorizaron artículos de revista arbitrada e indexados en Scopus o Web of Science; los preprints se incluyeron únicamente cuando contaban con DOI asignado y evidencia de envío a una revista Q1–Q3.

Los criterios de inclusión consideraron trabajos que abordaran explícitamente la intersección entre técnicas de IA/ML y al menos uno de los siguientes dominios: implementación o evaluación de algoritmos PQC, ataques o defensas de canal lateral sobre PQC, orquestación de migración quantum-safe y criptoanálisis asistido por IA. Se excluyeron artículos centrados exclusivamente en distribución cuántica de claves (QKD) sin cruce con PQC clásica, trabajos de divulgación sin metodología documentada y estudios anteriores a 2019 salvo referencias seminales con más de 50 citas en la literatura incluida. La síntesis se organizó temáticamente en torno a cinco ejes derivados de las preguntas de investigación, dado que la heterogeneidad de métricas y contextos de los estudios revisados hace inviable una síntesis cuantitativa unificada.

Fundamentos de la criptografía post cuántica

3.1. La amenaza cuántica sobre la criptografía clásica

Los criptosistemas asimétricos clásicos descansan sobre la dificultad computacional de problemas matemáticos específicos: la factorización de enteros grandes en RSA, el logaritmo discreto en Diffie-Hellman, y el logaritmo discreto sobre curvas elípticas en ECC (Al-Shabi, 2019). Estas dificultades resisten a cualquier adversario clásico con recursos polinomiales razonables. Sin embargo, el algoritmo cuántico de Shor (1994) reduce ambos problemas a tiempo polinomial cuando se ejecuta sobre un computador cuántico tolerante a fallos con suficientes qubits lógicos, mientras que el algoritmo de Grover proporciona una aceleración cuadrática en la búsqueda de claves simétricas, motivando la duplicación de los tamaños de clave AES (Mavroeidis et al., 2018; Sharbat, 2011) .

A lo anterior se suma el escenario harvest now, decrypt later (HNDL): adversarios estatales con capacidad de almacenamiento masivo pueden interceptar y archivar tráfico cifrado actualmente, a la espera de que la maduración del hardware cuántico les permita descifrarlo retroactivamente. Para datos con vida útil prolongada historias clínicas, secretos industriales, comunicaciones diplomáticas este vector convierte la migración a PQC en una urgencia inmediata, no diferida (Choudhury et al., 2025).

3.2 Familias matemáticas y estándares NIST

El concurso NIST clasificó las propuestas PQC en cinco familias matemáticas. La familia lattice-based se apoya en problemas como Learning With Errors (LWE), Module-LWE y Shortest Vector Problem (SVP) sobre retículas euclidianas; concentra los estándares ML-KEM y ML-DSA por su balance favorable entre tamaño de clave y rendimiento. Las criptografías code-based (McEliece, BIKE, HQC) explotan la dificultad de decodificación de códigos lineales con error; HQC fue seleccionada en 2025 como alternativa de encapsulamiento de clave. Las firmas hash-based (LMS, XMSS, SPHINCS+) derivan su seguridad únicamente de la resistencia a colisiones de funciones hash criptográficas, lo que las convierte en respaldo conservador frente a hipotéticos avances criptoanalíticos sobre retículas. Finalmente, los esquemas multivariate (Rainbow) e isogeny-based tuvieron un desempeño desigual y fueron parcialmente descartados (Balamurugan et al., 2021; Mahdi & A. Abdullah, 2025) .

La Tabla 1 sintetiza los estándares NIST publicados en 2024 y los borradores en curso, base indispensable para cualquier ejercicio de migración.

Estándar	Algoritmo base	Familia matemática	Aplicación principal	Categorías de seguridad
FIPS 203	ML-KEM (Kyber)	Lattice (Module-LWE)	Encapsulamiento de clave (KEM)	1, 3 y 5
FIPS 204	ML-DSA (Dilithium)	Lattice (Module-LWE/SIS)	Firma digital	2, 3 y 5
FIPS 205	SLH-DSA (SPHINCS+)	Hash-based	Firma digital (respaldo)	1, 3 y 5
FIPS 206 (borrador)	FN-DSA (Falcon)	Lattice (NTRU)	Firma compacta en entornos restringidos	1 y 5
En estandarización	HQC	Code-based (Hamming Quasi-Cyclic)	Encapsulamiento alternativo	1, 3 y 5

Tabla 1 Estándares NIST de criptografía post cuántica. Fuente: Elaboración propia

La elección entre familias depende del balance entre tamaño de clave, latencia de operación, requisitos de memoria y nivel de seguridad. ML-KEM ofrece claves públicas de aproximadamente 800 bytes en su nivel más bajo de seguridad y operaciones eficientes en hardware embebido, lo que explica su adopción como reemplazo predeterminado del intercambio de claves en TLS 1.3 en combinación con X25519. ML-DSA, en contraste, produce firmas de varios kilobytes, lo que tensiona protocolos de banda estrecha como ciertos perfiles de 5G NR (Choudhury et al., 2025; Demir et al., 2025).

Inteligencia artificial en la optimización e implementación de algoritmos PQC

La operativa de los algoritmos lattice-based introduce primitivas computacionales nuevas transformada teórica de números (NTT), muestreo gaussiano discreto, compresión polinomial que no estaban presentes en RSA o ECC. Estas operaciones, aunque matemáticamente seguras, presentan trade-offs no triviales en su implementación física, particularmente en plataformas con memoria escasa o restricciones energéticas estrictas. La IA ha demostrado ser una herramienta eficaz para navegar este espacio de diseño en cuatro líneas convergentes.

4.1. Optimización de parámetros mediante aprendizaje

Sobuj et al, presentaron un esquema lattice-based potenciado por aprendizaje automático que ajusta los parámetros de seguridad/rendimiento mediante optimización bayesiana, logrando reducciones medibles en el tiempo de generación de claves sin pérdida en el nivel de seguridad nominal (Sobuj et al., 2026). La optimización bayesiana resulta apropiada en este contexto porque cada evaluación de parámetros implica ejecutar un protocolo completo de cifrado y benchmarking, lo cual es costoso; los algoritmos evolutivos y

los métodos de búsqueda multi-objetivo basados en NSGA-II han mostrado resultados análogos en esquemas code-based (Yi, 2023). Una contribución destacable de esta línea es que los modelos de IA permiten explorar regiones del espacio de parámetros que las heurísticas humanas habían descartado, encontrando configuraciones Pareto-óptimas no triviales.

4.2. Reducción de overhead en entornos IoT y 5G

La integración directa de PQC en redes 5G y dispositivos del Internet de las Cosas enfrenta cuellos de botella severos. El cuello de botella SIB1 de 372 bytes en 5G NR, la fragmentación extensa que requieren los certificados ML-DSA de varios kilobytes y las sobrecargas energéticas prohibitivas en endpoints de baja potencia constituyen las fricciones arquitectónicas más documentadas (Do & Duong, 2026). Frente a este desafío, técnicas de IA se han propuesto para gestionar dinámicamente los trade-offs mediante marcos híbridos adaptativos: modelos de aprendizaje por refuerzo seleccionan en línea qué fragmentos del handshake comprimir, qué proporción de tráfico cifrar con esquemas híbridos clásico+PQC y cuándo conmutar entre niveles de seguridad NIST en función del estado de la batería y la calidad del enlace (Chen et al., 2025; Ghashghaei et al., 2024) .

Mahdi y Abdullah revisan exhaustivamente la combinación de PQC ligera y modelos compactos de aprendizaje automático para dispositivos con menos de 16 KB de RAM, destacando que la cuantización post-entrenamiento y la destilación de conocimiento permiten desplegar predictores de carga energética en microcontroladores ARM Cortex-M0+ junto con implementaciones reducidas de Kyber-512. Esta convergencia es particularmente relevante para aplicaciones médicas y agrícolas en el contexto latinoamericano (Mahdi & A. Abdullah, 2025).

4.3. Aceleración hardware asistida por IA

El diseño de coprocesadores y módulos FPGA para PQC mediante búsqueda automática de arquitecturas (Neural Architecture Search aplicado a hardware criptográfico) constituye una frontera emergente. Demir et al. (2025) reportan análisis de rendimiento e implementación industrial de algoritmos PQC en FPGAs Xilinx UltraScale+, mostrando que la exploración automatizada del espacio de microarquitecturas reduce el área ocupada (en términos de slices LUT) hasta en un 30% frente a diseños manuales para implementaciones equivalentes de ML-KEM, manteniendo la frecuencia operativa.

Ataques de canal lateral asistidos por inteligencia artificial sobre implementaciones PQC

Aunque los algoritmos PQC son matemáticamente seguros frente a adversarios cuánticos, sus implementaciones físicas constituyen una superficie de ataque distinta y crítica. Los ataques de canal lateral (side-channel attacks, SCA) extraen información sobre claves secretas mediante la observación de variables físicas del dispositivo durante la ejecución del algoritmo: consumo de potencia, emisiones electromagnéticas, tiempo de ejecución y radiación acústica o térmica. La IA, y en particular el aprendizaje profundo, ha transformado radicalmente este campo: los modelos neuronales automatizan la extracción de características de trazas físicas, eliminan la dependencia de modelos de fuga explícitos y reducen drásticamente el número de trazas necesarias para recuperar una clave secreta (Annadurai & Meenakshi, 2025; Delgado-Vargas et al., 2024).

5.1. Taxonomía de los SCA con IA sobre PQC

Los SCA asistidos por IA sobre implementaciones PQC pueden clasificarse según dos dimensiones complementarias. La primera es el canal físico explotado: análisis de potencia (DPA y CPA), análisis electromagnético (EMA), ataques temporales sobre implementaciones no constant-time, e inyección de fallos como clase complementaria activa. La segunda dimensión es la estrategia adoptada por el adversario, que se diferencia entre ataques con perfil (profiled) que requieren acceso previo a un dispositivo idéntico para entrenar un modelo, ataques sin perfil que automatizan CPA/DPA mediante IA, ataques de traza única que recuperan la clave a partir de una sola observación, y ataques horizontales que explotan correlaciones entre múltiples operaciones dentro de una misma traza (Ravi et al., 2024).

5.2. Ataques de aprendizaje profundo sobre ML-KEM (Kyber)

CRYSTALS-Kyber, estandarizado como ML-KEM (FIPS 203), es el algoritmo PQC más estudiado bajo SCA por su posición central en la migración quantum-safe. Kasture et al, demostraron que implementaciones FPGA sin contramedidas de los tres niveles de seguridad de Kyber (512, 768 y 1024) son comprometidas satisfactoriamente mediante DPA y CPA, con complejidad escalando linealmente con

el tamaño de la clave; el análisis de trazas de potencia a 500 MS/s con precisión de 12 bits permite recuperar la clave completa (Kasture et al., 2025).

La progresión hacia implementaciones protegidas no ha eliminado la amenaza. Ni et al, demostraron que un modelo CNN con conocimiento adicional del texto cifrado puede atacar cada coeficiente de 12 bits del vector de clave privada de Kyber utilizando tan solo 50 trazas, sin requerir conocimiento previo de la implementación ni del algoritmo (Ni et al., 2024). Ji y Dubrova extendieron estos resultados a implementaciones enmascaradas en hardware, recuperando la clave compartida mediante DL-SCA sobre la implementación enmascarada de primer orden, lo que evidencia la insuficiencia del enmascaramiento de bajo orden frente a adversarios DL (Ji & Dubrova, 2023).

En el contexto industrial del IoT, una evaluación comprehensiva de fugas en implementaciones de Kyber sobre ARM Cortex-M4 evaluó cuatro puntos de ataque con tres técnicas distintas bajo diversas combinaciones de contramedidas; los autores construyeron un modelo de aprendizaje profundo para cada punto de ataque, proporcionando una caracterización más precisa de la variabilidad de las trazas que la accesible mediante métodos estadísticos clásicos. Trabajos recientes del Queen's University Belfast presentan un ataque CPA mejorado en dos pasos sobre la implementación estándar de ML-KEM en ARM Cortex-M4, explotando el conocimiento de valores intermedios durante la multiplicación polinomial en la etapa de desencapsulamiento; el enfoque es genérico para todos los niveles de seguridad y extensible a otros esquemas lattice-based.

5.3. Ataques sobre ML-DSA (Dilithium)

CRYSTALS-Dilithium, estandarizado como ML-DSA (FIPS 204), presenta un punto de fuga particularmente sensible en el procedimiento de desempaquetado de la clave secreta (skDecode), primer paso del algoritmo de firma. Investigaciones presentadas en la 5ª Conferencia de Estandarización PQC del NIST en 2024 demuestran un ataque de traza única sobre la implementación C de Dilithium-2 en ARM Cortex-M4 (compilado con optimización -O3), explotando la fuga en skDecode mediante análisis de potencia profiled asistido por DL. El ataque recupera directamente los coeficientes de los polinomios del vector de clave secreta s1 y s2 sin requerir post-procesamiento extenso. Como contramedida, los autores proponen un esquema de enmascaramiento que divide s1 y s2 en dos shares durante la generación de claves, verificando que las funciones comprometidas dejan de filtrar bajo la implementación enmascarada (Ravi et al., 2024).

5.4. Evaluación de leakage y herramientas estandarizadas

La evaluación sistemática de la seguridad de las implementaciones PQC requiere herramientas estándar. La Evaluación de fugas en vectores de prueba (Test Vector Leakage AssessmentTVLA), prueba estadística basada en el test-t de Welch, detecta fuga en función de vectores de prueba fijos versus aleatorios y se aplica como primer paso en casi todos los trabajos revisados. La plataforma de hardware/software de código abierto ChipWhisperer es utilizada para captura de trazas y evaluación de SCA en múltiples trabajos sobre Kyber y Dilithium, permitiendo reproducibilidad de experimentos. Ganesh, Ahmed y Mady realizan una evaluación de fuga de orden superior y SCA basada en redes neuronales sobre la implementación enmascarada de primer orden de CRYSTALS-Kyber, demostrando que el enmascaramiento de primer orden es insuficiente frente a adversarios DL equipados con suficientes trazas (Ganesh et al., 2024).

5.5. Contramedidas y defensa adaptativa

Frente a la amenaza DL-SCA, la investigación en contramedidas ha evolucionado en dos líneas complementarias. La primera es el enmascaramiento booleano (Boolean masking), que divide variables sensibles en shares aleatorios; en Kyber requiere conversiones entre enmascaramiento aritmético y booleano debido a las operaciones de compresión modular, lo que introduce complejidad de implementación no trivial. El enmascaramiento de 4 bits proporciona un incremento de seguridad de aproximadamente 100× respecto a la implementación sin protección, al costo de mayor uso de slices FPGA y menor frecuencia máxima (Kasture et al., 2025) .

La segunda línea es la aleatorización temporal (shuffling), que reordena aleatoriamente las operaciones del algoritmo para romper correlaciones entre trazas. Xu et al, proponen una arquitectura de shuffling compacta para Kyber en FPGA basada en una versión modificada del algoritmo Fisher-Yates, verificando seguridad mediante CPA y TVLA (Xu et al., 2024). La combinación de enmascaramiento de orden superior con aleatorización temporal controlada constituye actualmente la mejor práctica documentada para implementaciones PQC en hardware embebido.

La investigación más reciente propone un giro epistémico: utilizar adversarios DL como herramienta misma de evaluación de seguridad, no solo como amenaza. Esta inversión genera perfiles de vulnerabilidad más realistas que los métodos estadísticos clásicos. Annadurai y Mennakshi presenta un framework para evaluación automatizada en el que un ensemble de modelos DL evalúa la efectividad de las contramedidas antes del despliegue, mientras que enfoques emergentes proponen aprendizaje por refuerzo (RL) para diseñar automáticamente contramedidas que maximicen la resistencia frente a SCA,

optimizando simultáneamente el trade-off seguridad–rendimiento (Annadurai & Meenakshi, 2025). La Tabla 2 sintetiza los trabajos clave revisados en este eje.

Autor	Algoritmo PQC	Técnica IA	Canal físico / Tipo	Resultado principal
(Kasture et al., 2025)	Kyber (ML-KEM)	DPA + CPA	Potencia (FPGA), sin perfil	Implementación sin protección comprometida; enmascaramiento 4 bits → mejora 100×
(Ni et al., 2024)	Kyber (ML-KEM)	CNN	Potencia (ARM), con perfil	50 trazas para recuperar clave privada
(Ji & Dubrova, 2023)	Kyber enmascarado	DL-SCA	Potencia (FPGA), con perfil	Clave recuperada de implementación enmascarada de 1er orden
(Wang et al., 2025)	Dilithium (ML-DSA)	DL profiled	Potencia (ARM Cortex-M4), traza única	Recuperación directa de s1, s2 vía skDecode
(Ganesh et al., 2024)	Kyber enmascarado	Red neuronal template	Potencia (ChipWhisperer), con perfil	1er orden insuficiente vs. DL en evaluación de orden superior
(Xu et al., 2024)	Kyber FPGA	CPA + TVLA (eval.)	Potencia (FPGA), defensa	Shuffling Fisher-Yates compacto verificado
(Aydin et al., 2021)	FrodoKEM, KEMs PQC	Análisis horizontal	Potencia, traza única	Vulnerabilidades horizontales en KEM/KEX poscuánticos
(Saeed & Alqahtani, 2026)	PQC + cifrado IoT	LSTM + RL	Tráfico de red, defensa adaptativa	Detección anomalías + RL + PQC en ecosistema IoT unificado

Tabla 2 Trabajos clave en ataques de canal lateral asistidos por IA sobre implementaciones PQC. Fuente: Elaboración propia

INTELIGENCIA ARTIFICIAL EN LA MIGRACIÓN Y ORQUESTACIÓN QUANTUM-SAFE

El plano de la migración a escala constituye el frente donde la IA tiene mayor impacto práctico inmediato. A diferencia de los planos algorítmico y de implementación, donde la investigación es predominantemente académica, la orquestación de la migración es ya un mercado activo: el segmento global de soluciones de migración PQC fue valorado en 15.000 millones de dólares en 2025, con una proyección de 86.500 millones para 2034 a una tasa de crecimiento anual compuesta del 22,0%, conforme reportan las consultoras del sector y los marcos institucionales como NCCoE SP 1800-38 (Hasan et al., 2023; Näther et al., 2024).

6.1. Descubrimiento y priorización automatizada de activos criptográficos

Las publicaciones de equipos de ingeniería de empresas con infraestructura masiva, como el blog técnico de Meta en 2026, reportan que el principal bloqueante de la migración no es el algoritmo, sino el inventario: identificar todos los activos criptográficos existentes certificados, claves, protocolos, APIs, equipos de tecnología operativa (OT) es una tarea de escala masiva que requiere automatización basada en IA. Herramientas como "Encryption Intelligence" de Arqit, lanzada comercialmente en enero de 2026 y seleccionada por el National Cyber Security Centre (NCSC) del Reino Unido, demuestran que la detección continua y la priorización por riesgo mediante IA son productos viables (Shaw, 2026).

6.2. Cripto-agilidad habilitada por IA

La cripto-agilidad capacidad de actualizar algoritmos criptográficos dinámicamente sin reingeniería arquitectónica constituye el marco dominante para la migración empresarial. Las plataformas de gestión de claves cripto-ágiles crecen aproximadamente al 26,3% anual dentro del mercado PQC. La IA actúa en tres puntos del ciclo: determina qué algoritmo emplear en cada contexto operativo, decide cuándo rotar claves de acuerdo con perfiles de riesgo dinámicos, y orquesta esquemas híbridos por ejemplo, ML-KEM combinado con X25519 en TLS 1.3 durante el periodo de transición clásico–post cuántico (Almuhammadi & Alghamdi, 2025; Olushola & Meenakshi, 2026).

6.3. Ingeniería de software asistida por IA (QSSE)

Zhang propone el marco AQuA (Automated Quantum-safe Adaptation) sobre tres pilares: detección de código PQC-aware, refactorización semántica automática y verificación híbrida. La brecha entre guías de alto nivel cripto-agilidad, evaluaciones de preparación y las herramientas de ingeniería de software constituye un área de investigación activa (Zhang, 2026). Los analizadores estáticos asistidos por modelos de lenguaje grandes (LLM-assisted static analysis) han demostrado capacidad para detectar usos heredados de RSA y ECC en bases de código de millones de líneas con precisión y exhaustividad (precision/recall) superiores a los analizadores basados en reglas (Shaw, 2026).

6.4. Marcos institucionales y escenarios de despliegue

El gobierno de Canadá, el NIST mediante NCCoE SP 1800-38, Europol y el Foro Económico Mundial (WEF) han publicado roadmaps y guías de migración que identifican la automatización y la IA como habilitadores críticos. Los plazos institucionales convergen: CNSA 2.0 fija 2030–2035 como horizonte de adopción obligatoria para sistemas federales estadounidenses, mientras que el NCSC británico recomienda

la transición completa para 2035 (Radanliev, 2024). Para el contexto de infraestructuras 5G/IoT, Do y Duong proponen un roadmap de cripto-agilidad en dos fases: transición híbrida durante 2025–2030 y soberanía PQC plena posterior a 2030, con la IA como capa transversal de orquestación (Do & Duong, 2026).

En aplicaciones específicas, Saeed y Alqahtani integran detección de anomalías basada en LSTM, aprendizaje por refuerzo y cifrado post cuántico en un framework de seguridad IoT unificado, demostrando que la detección de comportamiento anómalo en el canal de comunicación puede complementar las contramedidas físicas de los dispositivos. Esta convergencia de defensas en capas representa una de las direcciones más prometedoras para entornos críticos de salud digital, agricultura de precisión y manufactura conectada (Saeed & Alqahtani, 2026).

Inteligencia artificial como vector de ataque emergente

La aplicación de IA al criptoanálisis no es novedad: las redes neuronales han sido propuestas como herramientas de criptoanálisis sobre cifrados clásicos desde Rivest en 1991. Sin embargo, en el contexto PQC, la asimetría direccional cobra especial relieve: los métodos criptoanalíticos basados en aprendizaje resultan particularmente efectivos contra modelos basados en redes neuronales propuestos como primitivas criptográficas, lo que advierte contra propuestas recientes de "PQC neural networks" como sustituto directo de los esquemas matemáticos estandarizados (Mothukuri & Parizi, 2026).

Tres clases de amenaza requieren atención prospectiva. Primero, los ataques HNDL amplificados por IA: los modelos de aprendizaje pueden priorizar, clasificar y procesar grandes volúmenes de datos cifrados interceptados, maximizando el valor del descifrado diferido cuando los CRQC estén disponibles. Segundo, las vulnerabilidades durante la transición: los sistemas en migración que ejecutan simultáneamente algoritmos clásicos y PQC son superficies de ataque ampliadas, y la IA puede explotar configuraciones híbridas mal implementadas, particularmente fallos de downgrade en negociaciones TLS. Tercero, el red teaming automático: herramientas de IA para generación automática de exploits contra nuevas implementaciones PQC son una preocupación emergente, especialmente en la fase de transición donde los equipos de seguridad aún no dominan las características de los nuevos algoritmos (Marzougui et al., 2022).

Brechas de investigación y líneas futuras

El análisis sistemático de los trabajos revisados permite identificar brechas estructurales que delimitan la agenda de investigación inmediata. Una carencia estructural particularmente apremiante se relaciona con la ausencia de datasets públicos estándar para SCA-DL sobre PQC. A diferencia del conjunto de datos ASCAD, ampliamente adoptado para la evaluación de ataques de canal lateral sobre AES, no existe a la fecha un repositorio abierto y consensuado de trazas de potencia o emanaciones electromagnéticas correspondientes a implementaciones de ML-KEM/ML-DSA, lo que dificulta tanto la comparación reproducible entre métodos como la validación cruzada de las contramedidas propuestas. La construcción colaborativa de dicho recurso, idealmente bajo el auspicio del NIST o de un consorcio académico internacional, constituye una prioridad inmediata para el campo.

A esta limitación de infraestructura experimental se suma una cobertura desigual entre familias algorítmicas. La gran mayoría de los trabajos en SCA-DL se concentra en los esquemas lattice-based, particularmente Kyber y Dilithium, mientras que los esquemas hash-based (SLH-DSA/SPHINCS+) y code-based (HQC) han recibido atención considerablemente menor. Esta asimetría introduce un sesgo de evaluación con consecuencias potencialmente graves: en el escenario de que emergieran ataques criptoanalíticos no contemplados sobre lattice, las implementaciones SLH-DSA podrían convertirse en el reemplazo conservador, y la comunidad carece todavía de un retrato fino del perfil de fuga de estas alternativas.

En el plano metodológico persiste asimismo una exploración limitada de los ataques multi-canal y multi-modalidad. La práctica totalidad de los estudios revisados considera un único canal físico, pese a que los ataques que combinan dos canales típicamente potencia y emanaciones electromagnéticas, en el espíritu del marco SPERO han demostrado una efectividad notablemente superior en el contexto del cifrado clásico, sin que dicha ventaja haya sido suficientemente trasladada al ámbito de las primitivas PQC.

Una brecha de carácter normativo, no menos urgente, atañe a la evaluación formal frente a adversarios basados en aprendizaje profundo. Los estándares de evaluación actualmente vigentes TVLA y FIPS 140-3 no incorporan modelos de amenaza basados en DL en su perímetro de análisis, déficit reconocido por la propia comunidad investigadora. La consolidación de un benchmark estandarizado de evaluación que integre adversarios DL representaría, por tanto, una contribución de alto impacto industrial y regulatorio.

Un obstáculo de naturaleza distinta, pero igualmente determinante para la escalabilidad práctica tanto del ataque como de la defensa, lo plantea la transferibilidad de los modelos DL entre dispositivos —denominada en la literatura device portability problem. Los modelos entrenados sobre un dispositivo determinado raramente resultan aplicables de forma directa a otro sin reentrenamiento sustancial, situación que ha motivado el desarrollo incipiente de soluciones basadas en domain adaptation y transfer learning, todavía sin validación amplia en el contexto PQC.

Adicionalmente, la interpretabilidad (explainable AI, XAI) aplicada a criptografía permanece subexplorada. La mayoría de las defensas y análisis basados en IA usan modelos de "caja negra", lo que limita la adopción en entornos regulados, particularmente sectores financieros, sanitario y de defensa, donde la trazabilidad de las decisiones automatizadas es un requisito legal. Finalmente, la integración con blockchain, sistemas de votación electrónica e IA distribuida abre frentes nuevos: contratos inteligentes post-cuánticos, validadores PQC en blockchain y protección de modelos de IA entrenados con primitivas PQC son casos de uso emergentes con relevancia geopolítica creciente.

Discusión

Los hallazgos de la presente revisión coinciden con el diagnóstico de (Choudhury et al., 2025; Sakwa & Li, 2026) sobre la urgencia de la migración y el rezago de la cobertura PQC en infraestructuras críticas, pero matizan dichas posiciones en dos sentidos. En primer lugar, la literatura más reciente revela que la IA no es solo un acelerador del proceso de migración, sino un componente del nuevo paisaje de amenazas: los DL-SCA sobre Kyber y Dilithium han demostrado que el enmascaramiento de primer orden, considerado durante una década como contramedida suficiente para AES, es insuficiente frente a adversarios DL bien instrumentados (Ganesh et al., 2024; Ji & Dubrova, 2023). Esto contrasta con la

posición de (Zolfaghari & Koshiba, 2022),quienes proponían a la IA como un potenciador uniformemente positivo de la criptografía.

Los marcos institucionales de migración (NCCoE SP 1800-38, CNSA 2.0, NCSC) coinciden con los hallazgos académicos sobre la importancia del descubrimiento automatizado de activos, pero los superan en pragmatismo: las soluciones comerciales como Encryption Intelligence ya operan en entornos productivos, mientras que la academia mantiene un sesgo hacia la evaluación micro-arquitectónica de los algoritmos. Esta disociación entre los planos micro (algorítmico-implementación) y macro (orquestación-migración) es una característica saliente del campo y debe orientar el diseño de programas formativos para profesionales de ciberseguridad.

Conclusiones

La criptografía post cuántica ha transitado de tema teórico a problema urgente de ingeniería de sistemas, mientras que la inteligencia artificial se ha consolidado como habilitador transversal del proceso de migración quantum-safe. La presente revisión narrativa ha mapeado seis ejes temáticos en la intersección entre IA, PQC y migración, identificando hallazgos diferenciados en cada uno.

Los estándares NIST publicados en 2024 (FIPS 203, 204 y 205), junto con la selección continua de HQC y el borrador de FN-DSA, configuran el panorama operativo de la próxima década. La IA aporta un valor diferencial a la optimización paramétrica de las implementaciones PQC, sobre todo en entornos restringidos del IoT y la tecnología 5G, mediante la optimización bayesiana, la búsqueda automática de arquitecturas de hardware y el aprendizaje por refuerzo para la gestión adaptativa del compromiso entre seguridad y rendimiento. Los ataques de canal lateral asistidos por aprendizaje profundo han demostrado que el enmascaramiento de primer orden es insuficiente, por lo que son necesarias contramedidas combinadas (enmascaramiento de orden superior y shuffling) y un cambio epistémico que considere a los adversarios DL como herramienta de evaluación de la seguridad. La orquestación automatizada de la migración (descubrimiento de activos, criptorresiliencia e ingeniería de software PQC-aware) constituye el frente de mayor impacto industrial inmediato. La IA opera simultáneamente como una amenaza emergente a través de la amplificación HNDL, la explotación de transiciones híbridas y la red teaming automatizado.

Las brechas identificadas de ausencia de conjuntos de datos estándar reproducibles, sesgo hacia los algoritmos basados en mallas, evaluación formal insuficiente frente a adversarios de aprendizaje profundo, problema de portabilidad entre dispositivos e interpretabilidad limitada delimitan una agenda de investigación accionable. Para la comunidad académica latinoamericana, en particular, la convergencia de la PQC ligera, la IA compacta y el Internet de las cosas en sectores como la salud digital, la agricultura de precisión y la manufactura conectada representa una oportunidad de contribuir con ideas originales que tengan relevancia a nivel regional. Las líneas futuras de investigación incluyen la construcción colaborativa de un conjunto de datos abierto análogo a ASCAD para Kyber/Dilithium, la integración formal de adversarios de aprendizaje automático en estándares como FIPS 140-3 y la consolidación de marcos de criptorresistencia asistida por IA con métricas cuantitativas de madurez tecnológica.

Contribución de los autores

Todos los autores realizaron contribuciones sustanciales y equivalentes en todas las fases del trabajo, incluyendo la conceptualización del estudio, la búsqueda y curaduría bibliográfica, el análisis crítico de la literatura, la redacción del manuscrito y la revisión final. No hubo división jerárquica en el trabajo realizado, y cada autor colaboró de manera equitativa en la elaboración y presentación de los resultados y conclusiones del artículo.

Referencias bibliográficas

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., & Miller, C. (2025). Status report on the fourth round of the nist post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology.

Almuhammadi, S., & Alghamdi, S. (2025). A novel transition protocol to post-quantum cryptocurrency blockchains. Frontiers in Computer Science, 7, 1457000. https://doi.org/10.3389/fcomp.2025.1457000

Al-Shabi, M. A. (2019). A survey on symmetric and asymmetric cryptography algorithms in information security. International Journal of Scientific and Research Publications (IJSRP), 9(3), 576-589.

Annadurai, S., & Meenakshi, M. (2025). Artificial Intelligence Assisted Side-Channel Analysis: Security Assessment Challenges. 2025 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 1-5. https://doi.org/10.1109/WiSPNET64060.2025.11005231

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510. https://doi.org/10.1038/s41586-019-1666-5

Aydin, F., Aysu, A., Tiwari, M., Gerstlauer, A., & Orshansky, M. (2021). Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange and Encapsulation Protocols. ACM Transactions on Embedded Computing Systems, 20(6), 1-22. https://doi.org/10.1145/3476799

Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2021). Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions. Cryptography, 5(4), 38. https://doi.org/10.3390/cryptography5040038

Centellas Claros, L. S., Blanco Coca, L., & Sandoval Alcocer, J. P. (2022). Comparative study of the symmetric cryptography algorithms AES, 3DES and ChaCha20. 10(3), 283-302.

Chaganti, K. C. (2025). A Scalable, Lightweight AI-Driven Security Framework for IoT Ecosystems: Optimization and Game Theory Approaches. IEEE Access, 13, 72235-72247. https://doi.org/10.1109/ACCESS.2025.3558623

Chang, S.-Y., & Khan, Q. (2026). Post-Quantum Cryptography in Networking Protocols: Challenges, Solutions, and Future Directions. Cryptography, 10(1), 12. https://doi.org/10.3390/cryptography10010012

Chen, C.-L., Zeng, K.-W., Li, W.-Y., Lee, C.-F., Liu, L.-C., & Deng, Y.-Y. (2025). Lightweight Post-Quantum Cryptography: Applications and Countermeasures in Internet of Things, Blockchain, and E-Learning. ECEI 2025, 14. https://doi.org/10.3390/engproc2025103014

Choudhury, B., Hota, A., Karmakar, M., Saha, S., Nag, A., & Nandi, S. (2025). A Comprehensive Survey on Pre Versus Post Quantum Security Schemes for 5G-Enabled IoT Applications. IEEE Access, 13, 159305-159333. https://doi.org/10.1109/ACCESS.2025.3608623

Copeland, B. J. (2012). Turing: Pioneer of the information age (First Edition). Oxford University Press.

Delgado-Vargas, K. A., Mancillas-López, C., & Gallegos-García, G. (2024). A Look at Side Channel Attacks on Post-quantum Cryptography. Computación y Sistemas, 28(4). https://doi.org/10.13053/cys-28-4-5130

Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms (Versión 2). arXiv. https://doi.org/10.48550/ARXIV.2503.12952

Do, T. B., & Duong, M. T. (2026). From Harvest-Now-Decrypt-Later to Quantum-Safe 5G/IoT: Architectural Friction, Practical Mitigations, and a Cryptographic Agility Roadmap. SSRN. https://doi.org/10.2139/ssrn.6412508

Dooley, J. F. (2013). A Brief History of Cryptology and Cryptographic Algorithms. Springer International Publishing. https://doi.org/10.1007/978-3-319-01628-3

Dooley, J. F. (2024). History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms. Springer International Publishing. https://doi.org/10.1007/978-3-031-67485-3

Fernández, S. (2004). La criptografía clásica. Sigma: Revista de matemáticas, 119-142.

Ganesh, B., Ahmed, M., & Mady, A. (2024). Higher Order Leakage Assessment and Neural Network-based Attack on CRYSTALS-Kyber: Proceedings of the 21st International Conference on Security and Cryptography, 373-380. https://doi.org/10.5220/0012715700003767

Ghashghaei, F., Ahmed, Y., Elmrabit, N., & Yousefi, M. (2024). Enhancing the Security of Classical Communication with Post-Quantum Authenticated-Encryption Schemes for the Quantum Key Distribution. Computers, 13(7), 163. https://doi.org/10.3390/computers13070163

Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W., Gauravaram, P., & McKague, M. (2023). A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies. https://doi.org/10.48550/ARXIV.2307.06520

Hoffstein, J., Pipher, J., & Silverman, J. H. (2014). An Introduction to Cryptography. En J. Hoffstein, J. Pipher, & J. H. Silverman, An Introduction to Mathematical Cryptography (pp. 1-59). Springer New York. https://doi.org/10.1007/978-1-4939-1711-2_1

Ji, Y., & Dubrova, E. (2023). A Side-Channel Attack on a Masked Hardware Implementation of CRYSTALS-Kyber. Proceedings of the 2023 Workshop on Attacks and Solutions in Hardware Security, 27-37. https://doi.org/10.1145/3605769.3623992

Kasture, S., Maurya, S., Singh, A. P., Shukla, A., Kotiyal, A., & Mirza, K. (2025). Securing post-quantum cryptography: Side-channel resilience in CRYSTALS-Kyber key encapsulation mechanism. IAES International Journal of Artificial Intelligence (IJ-AI), 14(6), 5251. https://doi.org/10.11591/ijai.v14.i6.pp5251-5267

Mahdi, L. H., & A. Abdullah, A. (2025). Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography. Engineering, Technology & Applied Science Research, 15(2), 21812-21821. https://doi.org/10.48084/etasr.10141

Marzougui, S., Wisiol, N., Gersch, P., Krämer, J., & Seifert, J.-P. (2022). Machine-Learning Side-Channel Attacks on the GALACTICS Constant-Time Implementation of BLISS. Proceedings of the 17th International Conference on Availability, Reliability and Security, 1-11. https://doi.org/10.1145/3538969.3538980

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. https://doi.org/10.48550/ARXIV.1804.00200

Mothukuri, V., & Parizi, R. M. (2026). Securing Cryptography in the Age of Quantum Computing and AI: Threats, Implementations, and Strategic Response (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.2603.06969

Näther, C., Herzinger, D., Gazdag, S.-L., Steghöfer, J.-P., Daum, S., & Loebenberger, D. (2024). Migrating Software Systems towards Post-Quantum-Cryptography—A Systematic Literature Review. https://doi.org/10.48550/ARXIV.2404.12854

Ni, Z., Khalid, A., Liu, W., & O'Neill, M. (2024). Bitstream Fault Injection Attacks on CRYSTALS Kyber Implementations on FPGAs. 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE), 1-6. https://doi.org/10.23919/DATE58400.2024.10546550

Nitaj, A., & Rachidi, T. (2023). Applications of Neural Network-Based AI in Cryptography. Cryptography, 7(3), 39. https://doi.org/10.3390/cryptography7030039

Olushola, A., & Meenakshi, S. P. (2026). Design and implementation of an authenticated post-quantum session protocol using ML-KEM (Kyber), ML-DSA (Dilithium), and AES-256-GCM. Frontiers in Physics, 13, 1723966. https://doi.org/10.3389/fphy.2025.1723966

Pousa, A., Sanz, V. M., & De Giusti, A. E. (2011). Análisis de rendimiento de un algoritmo de criptografía simétrica sobre arquitecturas multicore. XVII Congreso Argentino de Ciencias de la Computación, 231-240.

Radanliev, P. (2024). Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, 15(1), 4. https://doi.org/10.1186/s40543-024-00416-6

Radanliev, P., Maple, C., & Santos, O. (2026). Complying with the NIST post-quantum cryptography standards and decentralizing artificial intelligence: Methodology for quantum-resistant and privacy-preserving digital identity systems. Frontiers in Blockchain, 8, 1702066. https://doi.org/10.3389/fbloc.2025.1702066

Ravi, P., Chattopadhyay, A., D'Anvers, J. P., & Baksi, A. (2024). Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results. ACM Transactions on Embedded Computing Systems, 23(2), 1-54.

Saeed, M. M. (2025). An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption. IEEE Access, 13, 104027-104036. https://doi.org/10.1109/ACCESS.2025.3576506

Saeed, M. M., & Alqahtani, F. (2026). AI and post-quantum cryptography powered cybersecurity approaches for IoT systems: A literature review. PeerJ Computer Science, 12, e3502. https://doi.org/10.7717/peerj-cs.3502

Sakwa, C. O., & Li, F. (2026). Survey on post-quantum cryptography implementations and deployment challenges. Computer Science Review, 61, 100975. https://doi.org/10.1016/j.cosrev.2026.100975

Sharbaf, M. S. (2011). Quantum cryptography: An emerging technology in network security. 2011 IEEE International Conference on Technologies for Homeland Security (HST), 13-19. https://doi.org/10.1109/THS.2011.6107841

Shaw, A. (2026). Quantum-Safe Code Auditing: LLM-Assisted Static Analysis and Quantum-Aware Risk Scoring for Post-Quantum Cryptography Migration (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.2604.00560

Sobuj, Md. A. M., Akter, S., Saha, G., Bhowmick, P. K., Kayes, I., & Sohan, Md. F. A. A. (2026). Machine Learning-Enhanced Lattice-Based Post-Quantum Cryptography for Security and Performance. En N. T. Nguyen, A.-C. Le, T. D. Tran, T.-P. Hong, Y. Manolopoulos, N. A. Le Khac, P. Tran Tin, & V.-N. Huynh (Eds.), Computational Intelligence in Engineering Science (Vol. 2945, pp. 197-211). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-21631-1_15

Wang, R., Gärtner, J., & Dubrova, E. (2025). Decompressing Dilithium's Public Key with Fewer Signatures Using Side Channel Analysis. 2025 IEEE 55th International Symposium on Multiple-Valued Logic (ISMVL), 135-140. https://doi.org/10.1109/ISMVL64713.2025.00034

Xu, D., Wang, K., & Tian, J. (2024). A Hardware-Friendly Shuffling Countermeasure Against Side-Channel Attacks for Kyber (Versión 5). arXiv. https://doi.org/10.48550/ARXIV.2407.02452

Yi, H. (2023). Machine Learning Method with Applications in Hardware Security of Post-Quantum Cryptography. Journal of Grid Computing, 21(2), 19. https://doi.org/10.1007/s10723-023-09643-4

Zhang, L. (2026). Toward Quantum-Safe Software Engineering: A Vision for Post-Quantum Cryptography Migration (Versión 2). arXiv. https://doi.org/10.48550/ARXIV.2602.05759

Zolfaghari, B., & Koshiba, T. (2022). AI Makes Crypto Evolve. Applied System Innovation, 5(4), 75. https://doi.org/10.3390/asi5040075