UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Dilithium en Criptografía Post-Cuántica

PROYECTO FIN DE GRADO

Daniel Linares Guerrero
Grado en Ingeniería de Software

Madrid, 2025

UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Grado en Ingeniería de Software

Dilithium en Criptografía Post-Cuántica

PROYECTO FIN DE GRADO

Daniel Linares Guerrero
Grado en Ingeniería de Computadores

Bajo la dirección de:
Dr. Giannicola Scarpa

Madrid, 2025

Título: Dilithium en Criptografía Post-Cuántica

Autor: Daniel Linares Guerrero

Grado en Ingeniería de Software

Dirección: Dr. Giannicola Scarpa

Abstract

Introduction and Motivation

Quantum computing poses a serious threat to classical cryptographic systems, especially those relying on problems like integer factorization and discrete logarithms. This growing risk has driven the development of post-quantum cryptography, aimed at safeguarding data confidentiality, integrity, and authenticity in a future where quantum computers are practically viable.

Objectives

The main goal of this thesis is to study the Dilithium digital signature algorithm, one of the schemes selected by NIST for standardization in the post-quantum era. The research covers its mathematical foundations, technical structure, comparative performance against traditional algorithms such as RSA and ECC, and a hands-on implementation in a real-world environment.

Findings

Dilithium is built upon lattice problems such as LWE (Learning With Errors) and SIS (Short Integer Solution), which remain intractable even with quantum capabilities. The algorithm offers a balance between performance and security, using medium-sized keys and moderately large signatures. Although signature sizes exceed those of ECC, the quantum-resistance it offers far outweighs this drawback.

Practically, Dilithium can be implemented on existing systems, including constrained devices, due to its efficient execution and low computational overhead. Furthermore, it integrates seamlessly into hybrid cryptographic models that combine classical and post-quantum mechanisms, enabling gradual migration without compromising security.

Conclusions

Dilithium stands out as a strong and efficient candidate for securing digital infrastructure against quantum threats. Its mathematical soundness, validated by NIST's standardization process, and its practical adaptability make it a compelling solution for future-proofing security systems. The conclusion is clear: early adoption of post-quantum cryptographic algorithms is not merely advisable, it is imperative to ensure long-term digital resilience.

Resumen

Introducción y Motivación

La computación cuántica amenaza los pilares de la criptografía clásica, basada en problemas como la factorización de enteros o logaritmos discretos. Esta vulnerabilidad ha impulsado el desarrollo de la criptografía post-cuántica, orientada a preservar la confidencialidad, integridad y autenticidad de la información en un escenario donde los ordenadores cuánticos sean una realidad práctica.

Objetivos

Este trabajo tiene como objetivo principal estudiar el algoritmo de firma digital Dilithium, uno de los estándares seleccionados por el NIST para resistir ataques cuánticos. El análisis incluye una descripción de sus fundamentos matemáticos, estructura técnica, ventajas frente a algoritmos clásicos como RSA o ECC y una implementación práctica en entorno real.

Hallazgos

Dilithium se basa en problemas de retículas como LWE (Learning With Errors) y SIS (Short Integer Solution), considerados intratables incluso con ordenadores cuánticos. Su diseño combina eficiencia y seguridad: utiliza claves de tamaño intermedio y firmas ligeramente más grandes que ECC, pero notablemente más seguras frente a amenazas cuánticas.

En cuanto a su implementación, se comprobó que puede integrarse en arquitecturas existentes, incluyendo dispositivos con recursos limitados, gracias a su rendimiento aceptable y bajo consumo computacional. Además, es compatible con esquemas híbridos que combinan criptografía clásica y post-cuántica, facilitando una transición progresiva sin comprometer la seguridad.

Conclusiones

Dilithium representa una solución robusta y eficiente frente a las amenazas emergentes de la computación cuántica. Su solidez matemática, reconocida por el proceso de estandarización del NIST, y su capacidad de adaptación a sistemas reales lo convierten en una opción viable para reforzar la seguridad en infraestructuras críticas. Se concluye que la adopción anticipada de algoritmos post-cuánticos es no solo recomendable, sino esencial para garantizar la continuidad y fiabilidad de los sistemas digitales en las próximas décadas.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Abreviaturas y Acrónimos

UPM	Universidad Politécnica de Madrid
PQC	Post-Quantum Cryptography
RSA	*Rivest–Shamir–Adleman*
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie–Hellman
EdDSA	Edwards-curve Digital Signature Algorithm
AES	Advanced Encryption Standard
TLS/SSL	Transport Layer Security / Secure Sockets Layer
MAC	Message Authentication Code
PKI	Public Key Infrastructure
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
DNI	Documento Nacional de Identidad
LWE	Learning With Errors
SIS	Short Integer Solution
SVP	Shortest Vector Problem
CVP	Closest Vector Problem
Qubit	Quantum Bit
BHT	Brassard–Høyer–Tapp
FFT	Fast Fourier Transform
QFT	Quantum Fourier Transform
NIST	National Institute of Standards and Technology
FIPS	Federal Information Processing Standards
ML-KEM	Module-Lattice Key Encapsulation Mechanism

EUF-CMA	Existential Unforgeability under Chosen Message Attack
OQS	Open Quantum Safe
OpenSSL	Open-Source SSL/TLS Toolkit
HSM	Hardware Security Module
IoT	Internet of Things
ARM	Advanced RISC Machine

1. ¿Qué problemas resuelve la criptografía?

1.1. Definición de criptografía

La criptografía es la disciplina que analiza métodos para resguardar la información y las comunicaciones a través del empleo de algoritmos matemáticos, de manera que solo aquellos con permiso y capacidad para descifrarlas puedan leerlas. En otras palabras, la criptografía oculta las comunicaciones para impedir que individuos no autorizados tengan acceso a ellas.

1.2. Principios básicos de la criptografía moderna

1.2.1. Confidencialidad

La privacidad es un principio fundamental de la seguridad de la información que asegura que solo los receptores autorizados tengan acceso a los datos. Para conseguirlo, se utilizan métodos de cifrado que transforman los datos en un formato ilegible para cualquier individuo que no tenga la clave correcta, protegiendo de esta manera el contenido de accesos no autorizados.

Un ejemplo de esta aplicación es el cifrado de archivos personales mediante el algoritmo AES, que impide que terceros puedan leer su contenido sin la clave correspondiente.

Entre los algoritmos más utilizados para preservar la privacidad se encuentran los métodos de cifrado simétrico, como AES y ChaCha20, que emplean una única clave para cifrar y descifrar los datos. También destacan los sistemas de cifrado asimétrico, como RSA y ECC, que utilizan un par de claves, una pública y otra privada, para asegurar comunicaciones seguras incluso en entornos abiertos. Estos mecanismos permiten asegurar que la información permanezca protegida frente a interceptaciones o filtraciones.

1.2.2. Integridad

La integridad es un principio fundamental en la seguridad de la información que garantiza que los datos no han sido alterados sin autorización. Para asegurar este objetivo, se utilizan funciones hash y códigos de autenticación que permiten verificar que la información recibida es exactamente la misma que la enviada, sin modificaciones intermedias.

Un ejemplo de aplicación de la integridad es el uso de checksums, como SHA-256, en la verificación de software. Este tipo de mecanismos permite confirmar que los archivos no han sido corrompidos o manipulados desde su distribución original.

Entre los algoritmos más comunes empleados para garantizar la integridad se encuentran las funciones hash, como SHA-256, SHA-3 y BLAKE2. Además, se utilizan códigos de autenticación de mensajes (MAC), destacando el algoritmo HMAC, que añade una capa de seguridad mediante el uso combinado de una clave secreta y una función hash. Estos métodos aseguran que cualquier intento de alterar los datos pueda ser detectado de forma inmediata.

1.2.3. Autenticación

La autenticación es un principio fundamental en la seguridad de la información que verifica la identidad de los usuarios o dispositivos en una comunicación, verificando que quien accede a un sistema es quien dice ser. Este proceso puede basarse en contraseñas, certificados digitales o métodos más robustos como la autenticación multifactor (MFA), que combina varios mecanismos de verificación.

Un ejemplo habitual es el uso de biometría, como la huella dactilar o el reconocimiento facial, en dispositivos móviles.

Para llevar a cabo la autenticación, se emplean protocolos como Kerberos y OpenID Connect, así como certificados digitales como X.509, gestionados a través de infraestructuras de clave pública (PKI), que proporcionan una base confiable para la validación de identidades.

1.2.4. No repudio

El no repudio es un principio fundamental en la seguridad de la información que garantiza que una parte no pueda negar haber llevado a cabo una acción o transacción. Este principio se asegura mediante el uso de firmas digitales, que vinculan de forma inequívoca a un usuario con una operación específica, proporcionando evidencia verificable de su autoría.

Un ejemplo claro es el registro de transacciones en tecnologías como Blockchain, donde cada operación queda firmada y registrada de forma inmutable.

Para implementar el no repudio, se emplean algoritmos de firma digital como RSA, ECDSA y Dilithium, este último diseñado para resistir ataques de la computación cuántica.

1.3. Ejemplos de aplicaciones reales

1.3.1. Seguridad en transacciones bancarias

Los bancos emplean la criptografía como una herramienta clave para proteger la información financiera de sus clientes y garantizar la seguridad de las operaciones.

En la banca online, se utiliza TLS/SSL para cifrar las comunicaciones entre el navegador del usuario y los servidores bancarios, evitando que los datos puedan ser interceptados por terceros. Además, se implementa autenticación multifactor para reforzar el acceso a las cuentas, combinando contraseñas con elementos adicionales como códigos enviados al móvil o datos biométricos.

Asimismo, en los pagos con tarjeta, el cifrado de datos a través del chip EMV asegura que la información sensible no pueda ser copiada ni reutilizada de forma fraudulenta. Estos mecanismos trabajan conjuntamente para salvaguardar tanto la integridad como la confidencialidad de las transacciones financieras.

1.3.2. Protección de datos en la nube

Empresas como Google, Microsoft o Amazon Web Services han convertido la criptografía en una pieza clave para proteger la información que almacenan sus usuarios en la nube. Esta protección no se limita a cifrar datos mientras se transfieren, sino que también abarca su almacenamiento, asegurando que incluso en reposo los datos permanezcan protegidos frente a accesos no autorizados.

Un aspecto crítico en este entorno es la gestión de claves, que se realiza mediante módulos físicos especializados conocidos como HSM (Hardware Security Modules). Estos dispositivos están diseñados para ofrecer un entorno seguro donde las claves pueden ser generadas, almacenadas y manipuladas sin riesgo de exposición. A su vez, las firmas digitales permiten validar que los archivos no han sido alterados, reforzando así la confianza en la integridad de los datos almacenados.

1.3.3. Aplicaciones en Blockchain y contratos inteligentes

Todo el ecosistema de las criptomonedas y los contratos inteligentes se apoya en estructuras criptográficas que permiten operar sin necesidad de confianza entre las partes. Desde la creación de una simple cartera de Bitcoin hasta la ejecución de complejos contratos en Ethereum, la seguridad depende de claves generadas mediante técnicas de cifrado que garantizan su unicidad y resistencia ante ataques.

Cada transacción, además, debe ir firmada digitalmente, lo cual no solo confirma que ha sido emitida por su propietario legítimo, sino que también impide su modificación una vez registrada. Este mecanismo ha hecho posible que las redes descentralizadas funcionen sin supervisión central, manteniendo la integridad del sistema a través de pura matemática.

1.3.4. Seguridad en dispositivos IoT

En el mundo del Internet de las Cosas, donde miles de dispositivos se conectan e intercambian datos constantemente, la criptografía también juega un papel fundamental. Muchos de estos dispositivos tienen recursos muy limitados, por lo que es necesario aplicar algoritmos de cifrado ligeros, como ChaCha20 o AES-GCM, que ofrezcan un equilibrio entre seguridad y eficiencia.

Pero cifrar los datos no es suficiente. Para establecer relaciones de confianza entre dispositivos y servicios, se utilizan certificados digitales que permiten autenticar a cada parte. Además, se adoptan medidas adicionales para evitar ataques en los que un tercero pueda interceptar o manipular la comunicación, como los conocidos ataques de tipo "Man-In-The-Middle".

1.3.5. Criptografía en comunicaciones militares y gubernamentales

Las agencias gubernamentales y las instituciones de defensa no pueden permitirse compromisos cuando se trata de seguridad. Por eso, la criptografía forma parte del núcleo de sus sistemas de comunicación. Radios encriptadas, redes privadas con cifrado de extremo a extremo y sistemas de autenticación basados en claves públicas son herramientas habituales en estos entornos.

En el caso de España, el DNI electrónico integra un chip criptográfico que permite realizar trámites online de forma segura, firmar documentos digitalmente y verificar identidades. Esta misma tecnología, adaptada a contextos más críticos, también se emplea en la protección de comunicaciones satelitales o en redes militares, donde cualquier filtración podría tener consecuencias graves.

2. Firmas Digitales

2.1. Firmas digitales: Concepto y aplicaciones

2.1.1. Definición y propósito

Las firmas digitales permiten verificar la autenticidad de un mensaje o documento digital. Funcionan de manera similar a una firma manuscrita, pero con un nivel de seguridad mucho mayor gracias al uso de criptografía asimétrica.

Objetivos principales:

- Autenticación: Verificar la identidad del remitente.
- Integridad: Garantizar que el mensaje no ha sido alterado.
- No repudio: Evitar que el remitente niegue haber firmado el mensaje.

2.1.2. Funcionamiento de una firma digital

Una firma digital se genera mediante criptografía de clave pública:

1. Generación de claves:
    - Se crean dos claves: una privada (para firmar) y una pública (para verificar).
2. Firma del mensaje:
    - Se calcula un hash del mensaje (H(m)).
    - El hash se cifra con la clave privada del firmante.
    - El resultado es la firma digital.
3. Verificación de la firma:
    - El receptor descifra la firma usando la clave pública del emisor.
    - Se compara el hash obtenido con el hash original del mensaje.
    - Si coinciden, la firma es válida.

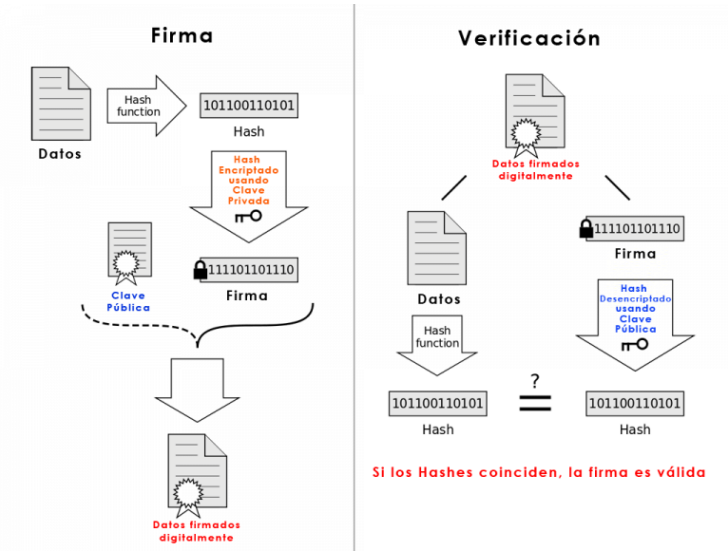

Ilustración 1. Funcionamiento firma digital.

2.1.3. Ejemplos de uso en el mundo real

- Certificados digitales (HTTPS, SSL/TLS): Verifican la identidad de sitios web.
- Firmas electrónicas en documentos legales.
- Protección de software y actualizaciones (firmware).
- Transacciones en Blockchain y criptomonedas.

2.2. Funciones de Hash importantes

2.2.1. Perspectiva Clásica

Las funciones hash criptográficas son esenciales para la protección de sistemas digitales, ofreciendo integridad de información, autenticación y respaldo para firmas digitales. En el enfoque tradicional, la seguridad de estas funciones se determina principalmente por su resistencia frente a ataques de choque y preimagen.

2.2.1.1. Ataque de Cumpleaños

El **ataque de cumpleaños** explota la paradoja del cumpleaños para encontrar colisiones en funciones hash. Matemáticamente, para una función hash con una salida de n bits, la probabilidad de encontrar una colisión alcanza el 50% después de aproximadamente $1.2 \times 2^{n/2}$ intentos. Por ejemplo, en una función hash de 128 bits, se necesitarían alrededor de 2^{64} intentos para encontrar una colisión, lo que destaca la necesidad de utilizar funciones hash con salidas más largas para mantener la seguridad adecuada.

Una **colisión** en una función hash ocurre cuando **dos entradas distintas** producen el **mismo valor hash**. Es decir, $H(m_1) = H(m_2)$ con $m_1 \neq m_2$.

2.2.1.2. Very Smooth Hash (VSH)

El **Very Smooth Hash (VSH)** es una función hash criptográfica diseñada para ser resistente a colisiones, basándose en problemas matemáticos difíciles, como encontrar raíces cuadradas modulares no triviales de números muy suaves. VSH es eficiente y adecuado para entornos con recursos limitados, como dispositivos embebidos, debido a su bajo requerimiento computacional. Sin embargo, su uso no es adecuado como sustituto de un oráculo aleatorio, pero puede ser útil en la construcción de funciones hash con trampa aleatorizadas.

Un número entero positivo n se dice **B-suave** si **todos sus factores primos son menores o iguales que B**. Por ejemplo:

- El número $60=2^2 \cdot 3 \cdot 5$ es 5-suave porque todos sus factores primos (2, 3 y 5) son ≤ 5.

2.2.2. Perspectiva Postcuántica

La computación cuántica introduce nuevos desafíos para la seguridad de las funciones hash, ya que ciertos algoritmos cuánticos pueden reducir significativamente la complejidad de ataques previamente considerados computacionalmente inviables.

2.2.2.1. Algoritmo de Grover

El **algoritmo de Grover** permite realizar búsquedas no estructuradas en una base de datos no ordenada con una complejidad de $O(2^{n/2})$, lo que implica que un ataque de **preimagen** contra una función hash de n bits puede realizarse en $O(2^{n/2})$ operaciones cuánticas. Esto reduce la seguridad efectiva de la función hash a la mitad de su tamaño de salida, lo que requiere el uso de funciones hash con salidas más largas para mantener la seguridad frente a adversarios cuánticos.

Un **ataque de preimagen** contra una función hash es un tipo de ataque criptográfico cuyo objetivo es **encontrar un mensaje de entrada que produzca un valor hash dado**.

2.2.2.2. Algoritmo de Brassard–Høyer–Tapp (BHT)

El **algoritmo de Brassard–Høyer–Tapp (BHT)** es un algoritmo cuántico diseñado para encontrar colisiones en funciones hash. Utiliza una combinación del algoritmo de Grover y técnicas de muestreo aleatorio para encontrar colisiones con una complejidad de $O(n^{1/3})$, lo que representa una mejora significativa sobre los métodos clásicos. Este algoritmo destaca la necesidad de considerar la resistencia a colisiones en el diseño de funciones hash en el contexto cuántico .

2.2.3. Comparaciones

Ataque / Algoritmo	Tipo	Objetivo	Complejidad (Clásica)	Complejidad (Cuántica)
Ataque de Cumpleaños	Clásico	Colisiones	$O(2^{n/2})$	$O(2^{n/3})$*
Very Smooth Hash (VSH)	Clásico	Resistencia a colisiones	Basado en problemas algebraicos difíciles	No aplica
Algoritmo de Grover	Cuántico	Preimagen	$O(2^{n})$	$O(2^{n/2})$
Algoritmo Brassard–Høyer–Tapp (BHT)	Cuántico	Colisiones	$O(2^{n/2})$	$O(2^{n/3})$

* La complejidad cuántica del ataque de cumpleaños con BHT es una estimación basada en resultados teóricos.

Tabla 1. Comparación ataques clásicos y cuánticos según su objetivo y complejidad.

3. Ejemplos de Criptografía Clásica: RSA y Curvas Elípticas

3.1. Algoritmo RSA

3.1.1. Introducción y contexto histórico

El algoritmo RSA, acrónimo de Rivest-Shamir-Adleman, fue introducido en 1977 como una solución criptográfica revolucionaria basada en la dificultad de factorizar números enteros grandes en sus factores primos. Esta propiedad matemática, conocida por su resistencia a la resolución mediante métodos computacionales clásicos, se convirtió en el pilar de uno de los primeros sistemas de cifrado de clave pública funcionales.

Desde su creación, RSA ha sido adoptado de forma masiva en múltiples áreas de la seguridad informática. Su doble capacidad para cifrar datos y generar firmas digitales lo ha posicionado como un estándar de facto en la protección de comunicaciones electrónicas, especialmente en el establecimiento de canales seguros y en la autenticación de identidades a través de certificados digitales. Hoy en día, continúa siendo empleado en protocolos críticos como TLS, en infraestructuras de clave pública y en sistemas de validación criptográfica que exigen confianza, integridad y confidencialidad.

3.1.2. Fundamentos matemáticos de RSA

RSA es un sistema de clave pública que utiliza dos claves:

- **Clave pública:** Se usa para cifrar los datos.
- **Clave privada:** Se usa para descifrar los datos y firmar digitalmente.

Generación de claves RSA:

1. Se eligen dos números primos grandes p y q.
2. Se calcula $n = p \times q$, que será el módulo de la clave pública y privada.
3. Se calcula la función de Euler $\phi(n) = (p - 1) \times (q - 1)$.
4. Se elige un número e tal que $1 < e < \phi(n)$ y que sea coprimo con $\phi(n)$.
5. Se calcula d como el inverso modular de e respecto a $\phi(n)$.
    - $d \times e \equiv 1 \bmod \phi(n)$

La clave pública es (n, e) y la clave privada es (n, d).

3.1.3. Funcionamiento del cifrado basado en RSA

- Cifrado:
  - Para cifrar un mensaje m, se usa la clave pública: $c = m^e \bmod$
  - El mensaje cifrado es c.
- Descifrado:
  - Se usa la clave privada para recuperar m: $m = c^d \bmod n$

3.1.4. Seguridad, aplicaciones y limitaciones del algoritmo RSA

El algoritmo RSA, ampliamente adoptado en entornos digitales, fundamenta su seguridad en la dificultad matemática de factorizar un número grande en sus dos factores primos. Esta operación, computacionalmente inviable mediante métodos clásicos cuando se emplean claves de tamaño adecuado, ha sido la base para su utilización en sistemas de cifrado, firmas digitales y autenticación segura a nivel global. No obstante, el panorama cambia radicalmente con la aparición de la computación cuántica, ya que algoritmos como el de Shor permiten factorizar enteros grandes en tiempo polinómico, comprometiendo directamente la robustez de RSA. Esta amenaza latente obliga a considerar cuidadosamente el tamaño de las claves utilizadas: mientras que una clave de 2048 bits sigue siendo considerada aceptable para el corto plazo, se recomienda utilizar longitudes de 3072 o incluso 4096 bits en escenarios donde la seguridad a medio y largo plazo sea crítica.

RSA se encuentra profundamente integrado en infraestructuras de seguridad modernas. Su uso es común en el cifrado de datos confidenciales durante conexiones seguras mediante protocolos como TLS o SSL, así como en la verificación de firmas digitales a través de certificados electrónicos bajo el estándar X.509. También se emplea en múltiples sistemas de autenticación y control de acceso, donde garantiza la identidad de las partes involucradas y la integridad de la información transmitida. Su versatilidad y soporte generalizado en bibliotecas criptográficas han contribuido a su adopción masiva durante las últimas décadas.

Sin embargo, no está exento de desventajas. Uno de los principales inconvenientes de RSA es su necesidad de utilizar claves de gran tamaño para mantener niveles adecuados de seguridad, lo que incrementa el coste computacional tanto en el cifrado como en la verificación de firmas. Además, su rendimiento es inferior al de algoritmos más modernos y ligeros, especialmente en dispositivos con recursos limitados. Finalmente, su vulnerabilidad frente a la computación cuántica lo posiciona como una solución cuya vigencia está cada vez más condicionada a los avances tecnológicos. Por esta razón, su uso debe ser evaluado con cautela en entornos donde la seguridad futura es un requisito estratégico.

3.2. Criptografía de Curvas Elípticas (ECC)

3.2.1. Introducción y contexto histórico

La criptografía de curvas elípticas, conocida por sus siglas en inglés como ECC (Elliptic Curve Cryptography), fue desarrollada a mediados de la década de 1980 como una alternativa más eficiente al algoritmo RSA. Su propuesta original planteaba un enfoque criptográfico que permitiera alcanzar niveles comparables de seguridad utilizando claves significativamente más pequeñas, lo cual la hacía especialmente atractiva para entornos con recursos limitados.

El principio matemático sobre el que se construye ECC es la dificultad de resolver el problema del logaritmo discreto en curvas elípticas (ECDLP, Elliptic Curve Discrete Logarithm Problem). Esta operación, incluso con los mejores algoritmos conocidos, resulta computacionalmente intratable cuando se trabaja con curvas adecuadamente seleccionadas y tamaños de clave apropiados. Esta resistencia frente a ataques conocidos, combinada con su eficiencia computacional, ha convertido a ECC en un estándar moderno dentro de la criptografía asimétrica.

En la actualidad, ECC se emplea de forma extensiva en diversas aplicaciones que requieren cifrado, generación de firmas digitales o establecimiento de claves compartidas seguras. Protocolos como ECDSA, ECDH o EdDSA, basados en curvas elípticas, han sido adoptados tanto en infraestructuras corporativas como en dispositivos móviles, servicios financieros y sistemas de comunicación cifrada.

3.2.2. Fundamentos matemáticos de ECC

ECC utiliza ecuaciones de curvas elípticas sobre cuerpos finitos. Una curva elíptica tiene la forma general:

$$y^2 = x^3 + a\,x + b$$

donde a y b son constantes que definen la curva.

- **Punto en la curva:** Cada punto en la curva tiene coordenadas (x,y).
- **Operación de suma de puntos:** Se define una operación que permite sumar dos puntos en la curva para obtener otro punto en la misma curva.
- **Multiplicación escalar:** Multiplicar un punto P por un número entero k genera un nuevo punto $Q = k\,P$.

El problema del logaritmo discreto en ECC consiste en encontrar k a partir de P y Q, lo que se considera computacionalmente difícil.

3.2.3. Funcionamiento del cifrado basado en ECC

El sistema de cifrado ECC sigue un esquema similar a Diffie-Hellman:

1. **Generación de claves:**
   - Se elige un número privado d.
   - Se calcula la clave pública como $Q=d\,P$, donde P es un punto fijo de la curva.
2. **Cifrado del mensaje:**
   - Se selecciona un número aleatorio k y se calcula $C_1 = k$ y $C_2=M + k\,Q$.
3. **Descifrado:**
   - Se usa la clave privada para recuperar M: $M = C_2 – d\,C_1$

3.2.4. Seguridad y aplicaciones de ECC

La criptografía de curvas elípticas destaca por ofrecer una elevada seguridad con claves de tamaño considerablemente más reducido en comparación con algoritmos como RSA. Una clave ECC de 256 bits proporciona un nivel de protección criptográfica equivalente al que se obtiene con una clave RSA de 3072 bits, lo que se traduce en mejoras significativas en eficiencia computacional, consumo energético y velocidad de procesamiento. Esta ventaja hace que ECC sea especialmente adecuada para entornos donde los recursos son limitados, como dispositivos móviles, tarjetas inteligentes o sistemas embebidos.

No obstante, al igual que ocurre con RSA, la seguridad de ECC se ve amenazada por el desarrollo de la computación cuántica. El algoritmo de Shor permite resolver el problema del logaritmo discreto en curvas elípticas en tiempo polinómico, lo que comprometería de forma directa su viabilidad en un escenario post-cuántico. Por esta razón, aunque ECC continúa siendo una solución robusta y eficiente en el contexto actual, su futuro depende de la evolución de alternativas resistentes al paradigma cuántico.

En cuanto a sus aplicaciones, ECC se encuentra ampliamente desplegada en múltiples sectores. Se utiliza de forma habitual en sistemas de cifrado para dispositivos móviles e Internet de las Cosas, donde la eficiencia y el bajo consumo son prioritarios. También tiene un papel fundamental en el ámbito de las criptomonedas, donde algoritmos como ECDSA son empleados para la generación y verificación de firmas digitales en redes como Bitcoin. Además, forma parte de los mecanismos de intercambio de claves en protocolos ampliamente adoptados como TLS, asegurando la confidencialidad de las comunicaciones en internet.

3.3. Comparación entre RSA y ECC

Característica	RSA	ECC
Seguridad base	Factorización de enteros	Logaritmo discreto en curvas elípticas
Tamaño de clave	3072 bits ≈ 256 bits ECC	Más pequeña y eficiente
Velocidad	Más lento	Más rápido
Uso en la actualidad	HTTPS, firmas digitales	Criptografía en móviles, Blockchain
Vulnerabilidad cuántica	Sí (algoritmo de Shor)	Sí (algoritmo de Shor)

Tabla 2. Comparación de parámetros entre RSA y ECC.

4. Criptografía Post-Cuántica y el Algoritmo Dilithium

4.1. Introducción a la Criptografía Post-Cuántica

4.1.1. Definición y objetivos

La criptografía post-cuántica, también conocida por sus siglas en inglés como PQC (Post-Quantum Cryptography), engloba un conjunto de algoritmos diseñados específicamente para resistir ataques ejecutados por ordenadores cuánticos. A diferencia de los sistemas criptográficos tradicionales como RSA o ECC, que quedarían obsoletos ante la capacidad del algoritmo de Shor para factorizar enteros y calcular logaritmos discretos de forma eficiente, los algoritmos post-cuánticos se fundamentan en problemas matemáticos que no pueden resolverse ni siquiera con el poder computacional proyectado para futuros sistemas cuánticos.

El primer objetivo esencial de esta nueva criptografía es garantizar la seguridad a largo plazo frente a amenazas cuánticas. Para ello, los algoritmos deben basarse en problemas que no se vean debilitados por los algoritmos cuánticos conocidos. Los principales enfoques actuales incluyen técnicas basadas en:

- Problemas de retículos (*lattice-based cryptography*)
- Códigos correctores de errores (*code-based cryptography*)
- Isogenias de curvas elípticas (*isogeny-based cryptography*)
- Funciones hash (*hash-based cryptography*)
- Sistemas multivariables (*multivariate polynomial cryptography*)

Cada uno de estos campos ofrece fundamentos matemáticos sólidos que resisten tanto ataques clásicos como cuánticos.

En paralelo, es imprescindible que los algoritmos post-cuánticos mantengan un rendimiento eficiente y práctico. La implementación debe ser viable en arquitecturas ya existentes, desde procesadores convencionales hasta dispositivos embebidos, tarjetas inteligentes y sistemas de red. Este criterio incluye no solo la velocidad de ejecución, sino también parámetros como el tamaño de las claves, la longitud de las firmas y el consumo de memoria. Además, la resistencia a ataques de canal lateral se considera un requisito de diseño indispensable en entornos reales.

Otro objetivo estratégico es facilitar una transición ordenada desde los sistemas criptográficos actuales. Se busca que los nuevos algoritmos puedan integrarse con un impacto mínimo en las infraestructuras, protocolos y APIs ya desplegados. Por este motivo, instituciones como el Instituto Nacional de Estándares y Tecnología (NIST) están liderando iniciativas de estandarización para evaluar no solo la seguridad teórica y práctica de los candidatos, sino también su facilidad de adopción.

También se considera prioritaria la interoperabilidad y la escalabilidad. Dado que la criptografía moderna está profundamente integrada en internet y en sistemas críticos globales, los nuevos esquemas deben ser compatibles con protocolos existentes como TLS, VPNs, certificados digitales y redes blockchain. La capacidad de adaptarse a un entorno de alta demanda y soportar millones de transacciones simultáneas sin degradación significativa del rendimiento es una condición imprescindible.

Por último, se reconoce que durante el periodo de adopción coexistirán sistemas clásicos y post-cuánticos. En este contexto, es fundamental que los algoritmos post-cuánticos puedan integrarse sin fricciones en entornos híbridos, donde se combinan firmas digitales o cifrados clásicos con mecanismos resistentes al paradigma cuántico. Esta convivencia debe reforzar la seguridad general sin introducir nuevas vulnerabilidades.

En conjunto, la criptografía post-cuántica no solo representa una respuesta técnica ante un desafío emergente, sino también una estrategia de continuidad y robustez frente a un futuro incierto en el que la computación cuántica podría reconfigurar por completo los cimientos de la seguridad digital.

4.1.2. Capacidades actuales de los ordenadores cuánticos

Aunque la computación cuántica ha registrado avances significativos en los últimos años, los sistemas disponibles siguen en una etapa preliminar de desarrollo. Su capacidad real todavía no permite aplicaciones comerciales de amplio alcance, y los retos técnicos continúan siendo notables. Para comprender su estado actual, conviene examinar varios factores clave que determinan su rendimiento y aplicabilidad.

Uno de los elementos fundamentales es la cantidad de qubits, que representan las unidades básicas de información cuántica. En 2025, compañías como IBM, Google y Honeywell han presentado procesadores que alcanzan entre 100 y 133 qubits. Un ejemplo destacado es el chip Heron de IBM, que incorpora 133 qubits con mejoras centradas en la fidelidad y la conectividad entre componentes. Sin embargo, estas cifras siguen estando muy por debajo de los millones de qubits que se estiman necesarios para ejecutar algoritmos complejos, como el de Shor, en escenarios prácticos.

La coherencia cuántica representa otro factor limitante. Se refiere a la capacidad de los qubits para mantener su estado cuántico sin que interfiera el ruido del entorno. Actualmente, esa coherencia tiene una duración muy breve, normalmente de unas pocas fracciones de milisegundo. Esta limitación impide la ejecución prolongada de algoritmos antes de que se degrade la información, lo que supone un obstáculo considerable para lograr cálculos precisos y sostenidos.

También resulta esencial considerar la fidelidad de las operaciones cuánticas, en particular de las puertas cuánticas, que actúan como mecanismos para manipular el estado de los qubits. Aunque las arquitecturas actuales permiten ejecutar secuencias básicas de operaciones, la precisión con la que se realizan sigue siendo insuficiente para garantizar resultados fiables en algoritmos exigentes. Cualquier error en estas operaciones puede propagarse a lo largo del circuito y comprometer completamente la ejecución.

La corrección de errores cuánticos constituye otra área crítica. Dado que los qubits son extremadamente sensibles a interferencias externas, se producen fallos de forma constante. Para corregir estos errores sin perder la información original, se recurre a códigos de corrección que requieren un gran número de qubits adicionales. Las estimaciones actuales indican que puede hacer falta entre mil y diez mil qubits físicos para estabilizar un único qubit lógico, lo que limita de forma evidente la viabilidad de los sistemas actuales.

Finalmente, la cuestión de la escalabilidad continúa siendo uno de los mayores retos de la computación cuántica. Aunque algunos procesadores han logrado aumentar el número de qubits disponibles, mantener la coherencia y asegurar una conectividad eficaz entre ellos se vuelve cada vez más complejo a medida que el sistema crece. En la mayoría de las arquitecturas actuales, no todos los qubits pueden interactuar directamente, lo que introduce cuellos de botella que frenan el rendimiento global. Por ello, la investigación se orienta a diseños modulares capaces de facilitar una expansión más controlada y eficiente.

En conjunto, aunque los progresos alcanzados son notables, los ordenadores cuánticos aún no disponen de la estabilidad, la fidelidad y la escala necesarias para realizar cálculos útiles en aplicaciones del mundo real. Se espera que la superación de estas limitaciones requiera aún una inversión sostenida de tiempo, investigación y recursos.

4.1.3. Avances recientes en hardware cuántico

El desarrollo del hardware cuántico ha experimentado un crecimiento notable en los últimos años, impulsado por iniciativas tanto del sector privado como de instituciones gubernamentales. Las investigaciones se han centrado en superar las limitaciones estructurales de los sistemas actuales, especialmente en lo que respecta a la estabilidad, escalabilidad y capacidad de interconexión de los qubits. En este contexto, varios actores clave han presentado innovaciones con un alto potencial disruptivo.

Microsoft ha dado un paso importante con la presentación de su chip cuántico conocido como Majorana 1. Este diseño se basa en una arquitectura topológica que utiliza partículas de Majorana para generar qubits significativamente más estables que los de tecnologías anteriores. La principal ventaja de este enfoque radica en su capacidad teórica para reducir la necesidad de corrección de errores mediante la protección inherente de los estados cuánticos. Según los desarrollos iniciales, este chip podría alojar hasta un millón de qubits en un formato compacto, y promete acelerar la resolución de ciertos problemas computacionales, reduciendo horizontes de décadas a solo unos años.

Por su parte, Cisco ha desarrollado un prototipo que apunta a resolver uno de los desafíos fundamentales en la computación cuántica: la conectividad entre dispositivos. Su propuesta consiste en un chip orientado a vincular ordenadores cuánticos de menor escala con sistemas más grandes, utilizando tecnologías de red convencionales combinadas con mecanismos de entrelazamiento cuántico. Este avance abre la posibilidad de establecer redes cuánticas distribuidas, capaces de sincronizar y coordinar múltiples nodos cuánticos en tiempo casi real.

En el ámbito internacional, China ha alcanzado hitos relevantes mediante el desarrollo de chips fotónicos cuánticos integrados. Uno de los logros más destacados ha sido la implementación del primer entrelazamiento cuántico multipartito utilizando variables continuas, directamente dentro del chip. Este tipo de arquitectura permite una mayor eficiencia en la transmisión y manipulación de información cuántica. Además, al integrar estos avances en dispositivos compactos, se allana el camino hacia la creación de redes cuánticas escalables y más fácilmente desplegables en entornos reales.

Estos desarrollos reflejan un esfuerzo global y coordinado por llevar la computación cuántica desde el laboratorio hacia entornos prácticos. Aunque aún queda un largo recorrido, los avances recientes en hardware cuántico están sentando las bases para una infraestructura tecnológica que podría redefinir los límites del procesamiento de información en las próximas décadas.

4.1.4. Algoritmo de Shor

El algoritmo de Shor, propuesto por Peter Shor en 1994, representa uno de los avances más trascendentales en el ámbito de la computación cuántica. Su objetivo principal es la factorización eficiente de números enteros, un problema que, bajo esquemas clásicos, requiere un tiempo subexponencial a medida que el tamaño del número aumenta. A diferencia de los algoritmos tradicionales, Shor permite realizar este proceso en tiempo polinómico, más concretamente en el orden de logaritmo de N al cubo, donde N es el número a factorizar. Esta capacidad pone en riesgo directo la seguridad de algoritmos criptográficos ampliamente utilizados como RSA, cuya robustez depende precisamente de la dificultad computacional de la factorización.

El algoritmo se articula en dos fases diferenciadas. En primer lugar, se realiza una etapa clásica en la que el problema de la factorización se transforma en el de encontrar el período de una función matemática determinada. Este paso permite reformular la tarea de forma que se vuelve accesible para el procesamiento cuántico. A continuación, se ejecuta la segunda fase, que es puramente cuántica. En ella, se emplea una computadora cuántica para identificar dicho período mediante la aplicación de la Transformada de Fourier Cuántica. Esta herramienta explota principios como la superposición y la interferencia para detectar patrones periódicos con una eficiencia imposible de replicar en sistemas clásicos. Una vez determinado el período adecuado, se pueden derivar los factores primos del número original con una alta probabilidad de éxito, completando así la tarea de forma eficaz.

Pese a la solidez teórica del algoritmo, su implementación práctica se enfrenta a limitaciones tecnológicas significativas. En 2021, investigadores de IBM lograron una prueba de concepto al factorizar el número 15 utilizando un procesador cuántico de apenas siete qubits. Aunque se trata de un ejemplo trivial, la experiencia sirvió para validar experimentalmente la lógica del algoritmo en un entorno físico real. Más recientemente, en abril de 2025, un estudio amplió los límites al explorar la aplicación del algoritmo de Shor en la factorización de cifras de hasta 4096 bits, bajo ciertas restricciones. Este avance fue posible gracias a mejoras en la eficiencia de los cálculos modulares y a la disminución en las tasas de error de chips cuánticos avanzados como el modelo Willow.

Sin embargo, el principal obstáculo para la factorización práctica de números grandes reside en los enormes requisitos de recursos que impone el algoritmo. Para procesar un número de 2048 bits, se calcula que serían necesarios entre diez y cien millones de qubits físicos, debido a la necesidad de implementar esquemas de corrección de errores. Actualmente, los ordenadores cuánticos comerciales operan con apenas unas pocas decenas o centenas de qubits, lo que deja claro que todavía falta un margen tecnológico considerable para que el algoritmo de Shor represente una amenaza real contra la criptografía moderna.

La corrección de errores cuánticos es, por tanto, una pieza esencial del rompecabezas. La inestabilidad inherente de los qubits, junto con su extrema sensibilidad al ruido y a las perturbaciones del entorno, hacen necesario utilizar códigos correctores que preserven la fidelidad de los cálculos. No obstante, estos mecanismos añaden complejidad al sistema y multiplican el número de qubits requeridos, retrasando aún más la posibilidad de desplegar el algoritmo de Shor en escenarios operativos. En consecuencia, aunque su potencial disruptivo es innegable, su amenaza concreta aún depende de la evolución futura del hardware cuántico.

4.1.5. Capacidad necesaria para romper RSA

El algoritmo de Shor, al ser implementado en un ordenador cuántico suficientemente potente, es capaz de factorizar números grandes y, por lo tanto, es capaz de romper sistemas criptográficos como RSA. Para descifrar una clave RSA de 2048 bits se calcular que serían necesarios cerca de 20 millones de qubits físicos, contando también con la necesidad de rectificar errores y la fiabilidad de las operaciones cuánticas.

Sin embargo, ciertas investigaciones proponen que, con avances en la eficiencia de los algoritmos y la fiabilidad de los qubits, este número se vería reducido de manera significativa. Por ejemplo, científicos de China han sugerido un modelo que podría romper RSA de 2048 bits con apenas 372 qubits, aunque este modelo ha generado discusiones y se considera teórico actualmente.

4.1.6. Proceso de estandarización del NIST

Dado el riesgo de los avances en computación cuántica, el **Instituto Nacional de Estándares y Tecnología (NIST)** lanzó en 2016 un proceso de selección de algoritmos post-cuánticos.

- **Fases del proceso:**
    1. **Convocatoria (2016)**: Se solicitaron propuestas de algoritmos resistentes a ataques cuánticos.
    2. **Evaluaciones y eliminaciones (2017-2023)**: Se analizaron aspectos como seguridad, eficiencia y facilidad de implementación.
    3. **Finalistas (2022):** Se seleccionaron **Kyber** (intercambio de claves) y **Dilithium y SPHINCS+** (firmas digitales).
    4. **Estándares oficiales (2024-2025):** El NIST formalizará las recomendaciones finales.

4.1.7. Ejemplos de algoritmos propuestos

4.1.7.1. Kyber: Mecanismo de Encapsulación de Claves Basado en Retículas

Kyber es un algoritmo de encapsulación de claves desarrollado en el marco del proyecto CRYSTALS (Cryptographic Suite for Algebraic Lattices), cuyo diseño responde a la necesidad urgente de mecanismos criptográficos resistentes al avance de la computación cuántica. Su fundamento matemático se basa en el problema del aprendizaje con errores (Learning With Errors, LWE) y su variante estructurada en módulos, conocida como Module-LWE. Estos problemas, ampliamente estudiados en la teoría de complejidad computacional, han demostrado ser intratables tanto para adversarios clásicos como cuánticos.

La solidez de Kyber ha sido reconocida formalmente por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), que lo ha seleccionado como el nuevo estándar para mecanismos de encapsulación de claves en entornos post-cuánticos. Esta designación, bajo la norma FIPS 203 y con el nombre técnico ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), posiciona a Kyber como una solución de referencia en la arquitectura de seguridad del futuro.

Uno de los elementos que han contribuido a su rápida adopción es su excelente relación entre nivel de seguridad y eficiencia. Frente a otros candidatos post-cuánticos, Kyber presenta tamaños de clave pública y de datos cifrados comparativamente reducidos, lo cual facilita su integración en infraestructuras reales sin generar penalizaciones significativas en rendimiento ni en consumo de recursos. En particular, la variante Kyber768 ofrece una seguridad equivalente a AES-192, con claves públicas de apenas 1.184 bytes y encapsulados de 1.088 bytes, parámetros operativos que permiten su uso incluso en contextos con limitaciones de ancho de banda o almacenamiento.

El despliegue práctico de Kyber ha avanzado de manera notable. Empresas líderes en tecnología y comunicaciones como Amazon Web Services y Signal han incorporado este algoritmo en sus sistemas para fortalecer la protección de sus canales de comunicación. A nivel técnico, su implementación ya está disponible en bibliotecas criptográficas reconocidas como liboqs y OpenSSL, lo que facilita su adopción por parte de desarrolladores en múltiples plataformas.

Cabe destacar, además, que el diseño de Kyber ha tenido en cuenta los riesgos asociados a ataques de canal lateral, una amenaza especialmente relevante en dispositivos embebidos y sistemas IoT. Se han desarrollado versiones endurecidas del algoritmo que incorporan contramedidas específicas para mitigar la exposición a filtraciones de información mediante análisis de tiempo, consumo o radiación electromagnética, garantizando así un nivel de seguridad adecuado en entornos de alta sensibilidad.

En términos de aplicabilidad, Kyber se configura como una herramienta esencial para el establecimiento de claves simétricas en protocolos críticos como TLS, VPNs o plataformas de mensajería cifrada. Su perfil técnico y su aval institucional lo convierten en un componente central dentro del ecosistema de criptografía post-cuántica, asegurando que las comunicaciones actuales puedan seguir siendo confidenciales y seguras frente a los retos tecnológicos del mañana.

4.1.7.2. SPHINCS+: Algoritmo de Firma Digital Basado en Árboles de Hash

SPHINCS+ es un esquema de firma digital sin estado, fundamentado en funciones hash criptográficas, diseñado específicamente para proporcionar una seguridad duradera frente a la amenaza que representa la computación cuántica. A diferencia de otros métodos de firma digital que dependen de problemas matemáticos como la factorización de números o el cálculo del logaritmo discreto, SPHINCS+ basa su fortaleza exclusivamente en la robustez de las funciones hash, las cuales han demostrado una resistencia notable ante diversos ataques criptográficos a lo largo del tiempo.

Este esquema ha sido reconocido y adoptado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) como uno de los estándares oficiales para firmas digitales post-cuánticas. Su característica de operar sin estado interno elimina los riesgos derivados de la gestión compleja de estados, tales como la reutilización accidental de claves privadas, un problema que puede comprometer la seguridad en sistemas tradicionales de firma.

SPHINCS+ ofrece un alto grado de flexibilidad mediante distintas configuraciones paramétricas que permiten ajustar el equilibrio entre el tamaño de las firmas generadas y los tiempos requeridos para su verificación. Esta adaptabilidad hace posible su implementación en una amplia gama de escenarios, donde pueden prevalecer diversas prioridades entre eficiencia y seguridad.

En cuanto a las dimensiones, las firmas generadas por SPHINCS+ suelen ser significativamente mayores en comparación con otros esquemas criptográficos, con tamaños que pueden alcanzar aproximadamente 16 kilobytes en niveles altos de seguridad. No obstante, las claves públicas y privadas mantienen un tamaño moderado, lo que facilita su almacenamiento, distribución y gestión en infraestructuras digitales.

En la práctica, SPHINCS+ ya está disponible en varias bibliotecas criptográficas de renombre, y se han desarrollado versiones optimizadas para diferentes entornos, incluyendo dispositivos con recursos limitados, tales como sistemas embebidos o hardware de baja potencia. Esta versatilidad incrementa su potencial para ser integrado en soluciones reales, garantizando la protección de la integridad y autenticidad de la información.

Este algoritmo resulta especialmente valioso en contextos donde la seguridad a largo plazo es un requisito ineludible, como puede ser la firma de firmware, la emisión de certificados digitales o la validación de documentos legales. SPHINCS+ asegura que estos procesos mantengan su validez y resistencia frente a adversarios que podrían disponer en el futuro de capacidades computacionales cuánticas avanzadas, protegiendo así activos digitales esenciales en la era post-cuántica.

4.1.7.3. Comparativa entre algoritmos post-cuánticos seleccionados por NIST

Algoritmo	Tipo	Base matemática	Tamaño clave pública	Tamaño firma / mensaje cifrado	Velocidad (sign/verify o encaps/decaps)	Seguridad cuántica	Estado NIST
Kyber	KEM (Intercambio de claves)	Retículas (Module-LWE)	800 - 1.184 bytes	768 - 1.088 bytes	Muy alta (cifrado/descifrado rápido)	Alta	**Estándar (FIPS 203)**
Dilithium	Firma digital	Retículas (Module-LWE y Module-SIS)	1.312 - 1.792 bytes	2.420 - 2.700 bytes (firma)	Alta (firma y verificación rápidas)	Alta	**Estándar (FIPS 204)**
SPHINCS+	Firma digital	Árboles de hash	32 - 64 bytes	7.856 - 17.136 bytes (firma)	Baja (verificación lenta, firmas grandes)	Muy alta (conservador)	**Estándar (FIPS 205)**

Tabla 3. Comparación entre algoritmos post-cuánticos.

4.2. Fundamentos Matemáticos de Dilithium

4.2.1. Problema de Redes Euclidianas

La base teórica sobre la que se construye Dilithium está profundamente ligada a la dificultad de ciertos problemas definidos sobre redes euclidianas, también conocidas como lattices. Estas estructuras pueden imaginarse como conjuntos discretos de puntos distribuidos regularmente en un espacio de n dimensiones, generados a partir de combinaciones lineales enteras de vectores base. Aunque conceptualmente sencillas, las operaciones matemáticas que implican estas redes presentan una complejidad considerable cuando se trabaja en dimensiones elevadas.

Uno de los problemas centrales en este marco es el denominado Shortest Vector Problem (SVP), que plantea la búsqueda del vector no nulo más corto dentro de una red dada. A pesar de que el enunciado del problema es directo, su resolución es altamente compleja: encontrar una solución exacta es un problema NP-hard, y ni siquiera existen algoritmos eficientes que proporcionen buenas aproximaciones cuando se escala la dimensión. Lo especialmente relevante en este contexto es que esta dificultad persiste incluso ante el uso de computación cuántica, lo que posiciona al SVP como una barrera robusta frente a amenazas futuras.

En el contexto de Dilithium, esta propiedad se explota para garantizar la seguridad del sistema. El diseño del esquema se basa en estructuras que hacen que calcular vectores cortos, o incluso razonablemente cercanos al mínimo, sea tan complejo como resolver el SVP en su forma más general. Esto significa que comprometer una firma o reconstruir una clave sin autorización exigiría resolver un problema que se considera inabordable con los recursos computacionales actuales y previsibles.

4.2.2. Problema del Aprendizaje con Errores (LWE)

Otro componente fundamental del andamiaje criptográfico de Dilithium es el problema de Aprendizaje con Errores, más conocido por sus siglas en inglés: LWE (Learning With Errors). Esta formulación moderna introduce un enfoque diferente: se plantea la resolución de sistemas de ecuaciones lineales, pero contaminados con un pequeño margen de error aleatorio. La dificultad no reside en la parte lineal, sino precisamente en ese ruido, que hace que recuperar la información original sea computacionalmente inviable.

Formalmente, se parte de una matriz pública A, un vector secreto s y un vector de error e. A partir de estos, se genera un vector de salida b tal que:

$$A \cdot s + e = b \bmod q$$

A simple vista, podría parecer un sistema resoluble, pero el pequeño error introducido en e es suficiente para romper cualquier intento de invertir el proceso sin acceso directo a s.

Desde el punto de vista teórico, LWE ha demostrado ser tan complejo como los problemas más duros en el dominio de redes euclidianas, incluyendo SVP o GapSVP, lo cual se ha probado mediante reducciones polinómicas. En la práctica, esto implica que, si alguien lograra romper LWE, también podría resolver los grandes problemas abiertos en lattices, lo cual se considera extremadamente improbable, incluso bajo el modelo cuántico.

En Dilithium, LWE se utiliza como base para la generación de claves públicas seguras. El ruido introducido actúa como un mecanismo de protección, impidiendo que un atacante pueda deducir la clave privada a partir de la clave pública. Este enfoque proporciona resistencia no solo frente a ataques clásicos, sino también ante posibles avances en computación cuántica.

4.2.3. Problema Short Integer Solution (SIS)

El tercer gran bloque matemático en el que se apoya Dilithium es el problema Short Integer Solution (SIS). Su formulación es también sencilla en apariencia: encontrar un vector entero distinto de cero, denominado z, tal que:

$$A \cdot z = 0 \bmod q$$

y además que la norma de z sea lo más pequeña posible. Al igual que en LWE, la matriz A es pública, y q representa un módulo primo predefinido.

Lo que hace especialmente interesante al problema SIS es que, al igual que LWE, su complejidad ha sido vinculada teóricamente a los problemas más difíciles dentro de la teoría de lattices. Hasta la fecha, no se ha descubierto ningún algoritmo, ni clásico ni cuántico, que permita resolver SIS de forma eficiente en dimensiones elevadas con parámetros bien elegidos. Esta solidez matemática lo convierte en una base muy atractiva para sistemas criptográficos post-cuánticos.

Dentro de Dilithium, SIS se utiliza para garantizar propiedades esenciales en las firmas digitales, como la unicidad y la no falsificación. En concreto, la dificultad de generar dos firmas distintas válidas para el mismo mensaje (colisiones) está directamente ligada a la intractabilidad del problema SIS. Así, este componente actúa como un ancla criptográfica que refuerza la autenticidad y la integridad del esquema de firma frente a ataques de reutilización o manipulación.

4.3. Estructura del Algoritmo Dilithium

El algoritmo Dilithium pertenece a la familia de esquemas de firma digital basados en redes euclidianas (*lattice-based cryptography*), y específicamente está construido sobre las estructuras del problema Module-LWE y Module-SIS, que permiten un balance óptimo entre eficiencia, compacidad y seguridad post-cuántica. La estructura se divide en tres fases principales: generación de claves, firma de mensajes y verificación de firmas.

4.3.1. Generación de Claves

La generación de claves en Dilithium implica el uso de estructuras algebraicas sobre anillos polinomiales y la incorporación controlada de ruido para asegurar seguridad criptográfica.

1. **Selección de parámetros**:
   - Se define un módulo primo q, un grado n para los polinomios, y dimensiones del módulo k y l para matrices polinómicas.
   - Se generan dos vectores de polinomios cortos aleatorios: $s_1 \in R_l$ y $s_2 \in R_k$, donde $R = \mathbb{Z}_q[x]/(x^n + 1)$.
   - Se introducen errores controlados mediante muestreo discreto, típicamente con una distribución centrada y estrecha (e.g., gaussiana o uniforme limitada) para preservar la compacidad y resistencia al análisis.
2. **Cálculo de la clave pública y privada**:
   - **Clave privada**: Está compuesta por los vectores s_1, s_2 y una semilla secreta para regenerar la matriz pública A.
   - **Clave pública**: Se construye como $t = A \cdot s_1 + s_2 \bmod q$, donde A es una matriz generada pseudodeterminísticamente a partir de una semilla pública. Se aplica un redondeo al vector t para generar una versión truncada t_1, que junto con la semilla forma la clave pública.
   - Este diseño impide que la clave privada pueda ser inferida a partir de la clave pública, debido a la dureza del problema Module-LWE.

4.3.2. Firma de Mensajes

El proceso de firma en Dilithium garantiza la unicidad, no repudio y resistencia a ataques adaptativos mediante un diseño determinista con aleatoriedad interna.

1. **Generación del vector aleatorio**:
   - Se selecciona un vector aleatorio $y \in R_l$, con elementos cortos, utilizando una fuente pseudoaleatoria derivada del mensaje y la clave privada. Este vector actúa como una preimagen criptográfica que oculta la firma durante la verificación.
2. **Cálculo del compromiso criptográfico**:
   - Se calcula $w = A \cdot y \bmod q$, se redondea y se aplica un hash sobre el resultado junto con el mensaje para obtener un desafío determinista c (mediante un *random oracle* como SHAKE-256).

3. **Ajuste con la clave privada**:
    - Se calcula $\mathbf{z} = \mathbf{y} + \mathbf{c} \cdot \mathbf{s}_1$, asegurando que $\mathbf{z}$ permanezca dentro de un rango aceptable para evitar fugas de información.
    - Se ejecuta un proceso de rechazo (*rejection sampling*) para garantizar que la distribución estadística de las firmas no revele correlaciones explotables sobre $\mathbf{s}_1$.
4. **Generación de la firma**:
    - La firma final consiste en el par $(\mathbf{z}, \mathbf{c})$ y un *hint* adicional que permite al verificador reconstruir parcialmente el compromiso $\mathbf{w}$ sin necesidad del vector $\mathbf{y}$ original, manteniendo eficiencia y compacidad.

4.3.3. Verificación de Firmas

La verificación es determinista y se basa en propiedades algebraicas de la estructura del anillo y las redes subyacentes.

- **Reconstrucción del compromiso**:
    - A partir de $\mathbf{z}$ y del desafío $\mathbf{c}$, el verificador reconstruye una estimación del vector $\mathbf{w'} = \mathbf{A} \cdot \mathbf{z} - \mathbf{c} \cdot \mathbf{t}_1 \bmod \mathbf{q}$, utilizando solo la clave pública y la firma.
    - Se utiliza el *hint* incluido para afinar el proceso de redondeo y recuperar la representación original.
- **Validación matemática**:
    - Se verifica que $\mathbf{z}$ se mantenga dentro de las normas permitidas (i.e., que sea "corto" en norma infinita), y que el hash del nuevo compromiso y del mensaje coincida con el desafío $\mathbf{c}$.
    - Esta validación garantiza que la firma fue efectivamente producida con el conocimiento de la clave privada asociada a la clave pública.
- **Seguridad**:
    - El proceso impide la reutilización de firmas (protección contra *replay attacks*) y la forja de nuevas firmas válidas para mensajes no firmados, incluso ante adversarios con capacidades cuánticas.

4.4. Seguridad de Dilithium

4.4.1. Propiedades de resistencia frente a ataques cuánticos

Uno de los pilares más sólidos de Dilithium como esquema criptográfico post-cuántico es su resistencia intrínseca frente a ataques llevados a cabo mediante computación cuántica. Esta fortaleza no es circunstancial, sino que se basa en fundamentos matemáticos profundamente estudiados: en concreto, en la complejidad computacional de problemas definidos sobre redes euclidianas, como el Shortest Vector Problem (SVP) y el Closest Vector Problem (CVP). Ambos se consideran inabordables incluso cuando se dispone de tecnología cuántica avanzada, debido a su naturaleza algebraicamente resistente.

Una de las principales garantías de seguridad es la inmunidad al algoritmo de Shor, una de las amenazas más relevantes en el contexto post-cuántico. Mientras que Shor es capaz de romper criptosistemas tradicionales basados en la factorización de enteros (como RSA) o logaritmos discretos (como ECC), no puede aplicarse a los problemas estructurales sobre los que se construye Dilithium. Las redes euclidianas no permiten transformaciones que reduzcan su resolución a tiempo polinómico mediante este tipo de algoritmos.

Además, hasta el momento no se ha descubierto ningún algoritmo cuántico eficiente, ni siquiera en el plano teórico, que permita resolver SVP o CVP en tiempos subexponenciales. Es cierto que algoritmos como el de Grover podrían mejorar ataques de fuerza bruta mediante una aceleración cuadrática, pero este impacto es fácilmente compensable ajustando los parámetros de seguridad del sistema (por ejemplo, aumentando el tamaño de las claves o la dimensión de las redes utilizadas).

Por último, Dilithium ha sido desarrollado y analizado dentro de modelos de seguridad bien definidos, como el EUF-CMA (Existential Unforgeability under Chosen Message Attack), lo que implica que su diseño contempla escenarios en los que un adversario puede elegir mensajes arbitrarios para intentar forzar colisiones o firmas válidas. Las evaluaciones realizadas por el NIST en el proceso de estandarización PQC han demostrado que el esquema resiste tanto ataques clásicos como cuánticos bajo hipótesis realistas.

En conjunto, Dilithium se posiciona como una solución robusta frente al paradigma post-cuántico, alineándose con los requisitos de seguridad de largo plazo que exige la infraestructura crítica moderna. Su diseño no solo resiste las amenazas actuales, sino que anticipa con criterio técnico los posibles vectores de ataque emergentes en el futuro cuántico.

4.4.2. Análisis de Eficiencia y Tamaño de Claves

Dilithium ha sido diseñado con una arquitectura equilibrada que permite su aplicación tanto en sistemas embebidos con recursos limitados como en grandes infraestructuras donde el rendimiento y la escalabilidad son factores clave. Su enfoque práctico combina resistencia criptográfica post-cuántica con costes computacionales razonables, lo que lo convierte en una alternativa sólida frente a esquemas tradicionales como RSA o ECC.

Uno de los aspectos más destacados es el tamaño de sus claves y firmas. Las claves públicas de Dilithium varían entre 1.3 KB y 1.5 KB, mientras que las firmas se sitúan entre 2.4 KB y 2.7 KB, en función del nivel de seguridad elegido (Dilithium II, III o V). Si bien estas cifras representan un incremento notable respecto a los tamaños compactos de ECC, lo cierto es que reflejan un compromiso aceptable si se considera la ganancia en resistencia frente a ataques cuánticos.

Desde el punto de vista computacional, Dilithium no recurre a operaciones complejas o costosas, sino que se apoya en aritmética modular y transformadas discretas (como la FFT), lo que facilita implementaciones eficientes. De hecho, en desarrollos optimizados sobre arquitecturas comunes, como procesadores ARM o implementaciones en lenguaje C, el algoritmo muestra tiempos de generación y verificación de firmas competitivos, en especial en procesos de validación masiva.

Además, su bajo consumo de recursos lo hace adecuado para dispositivos con restricciones severas, como tarjetas inteligentes, firmware de bajo nivel o sensores IoT. A diferencia de otros esquemas que requieren hardware especializado o aceleradores criptográficos, Dilithium puede desplegarse en entornos legacy sin reestructuración drástica, lo que facilita la transición hacia sistemas resistentes al paradigma cuántico.

En términos comparativos, aunque sus firmas son más grandes que las de ECC, sus claves públicas y privadas resultan mucho más pequeñas que las utilizadas por RSA para alcanzar niveles de seguridad equivalentes. Este detalle cobra especial relevancia en entornos distribuidos donde el almacenamiento, la transmisión y la gestión de claves son factores críticos, como en protocolos TLS, DNSSEC o aplicaciones blockchain.

En conjunto, Dilithium logra un equilibrio entre solidez criptográfica, eficiencia operativa y viabilidad de integración. Su adopción está plenamente justificada en escenarios donde la seguridad a largo plazo no es un valor añadido, sino un requisito estratégico.

4.4.3. Comparación con Firmas Clásicas (RSA y ECC)

Característica	RSA	ECC	Dilithium
Seguridad	Vulnerable a computadoras cuánticas	Vulnerable a computadoras cuánticas	Seguro ante ataques cuánticos
Tamaño de clave	Grande (3072 bits)	Pequeño (256 bits)	Intermedio
Velocidad	Lento	Rápido	Más eficiente que RSA

Tabla 4. Comparación de Dilithium con Firmas Digitales Clásicas.

4.5. Criptografía Híbrida

En el proceso de transición hacia una infraestructura criptográfica resistente a la computación cuántica, una estrategia cada vez más adoptada es el uso de sistemas híbridos. Estos sistemas combinan algoritmos criptográficos clásicos, como RSA o ECC, con esquemas post-cuánticos como Dilithium o Kyber, con el objetivo de ofrecer una capa adicional de seguridad y asegurar la compatibilidad con los estándares existentes.

La motivación detrás del enfoque híbrido radica en la necesidad de mantener la interoperabilidad con sistemas legados al mismo tiempo que se introduce resiliencia frente a ataques que, en un futuro cercano, podrían ser viables mediante computadoras cuánticas. En lugar de reemplazar completamente los algoritmos actuales, el modelo híbrido permite que tanto los métodos clásicos como los nuevos coexistan dentro de un mismo protocolo o arquitectura, protegiendo los datos incluso si uno de los algoritmos llegara a quedar comprometido.

Por ejemplo, en el caso de las firmas digitales, ya se han desarrollado implementaciones que integran esquemas como RSA o ECDSA junto con Dilithium. En estas configuraciones, una operación de firma genera dos firmas simultáneamente, cada una correspondiente a un algoritmo distinto, y ambas deben ser verificadas para considerar válida la autenticación. Esta técnica ofrece una garantía dual: mantiene la compatibilidad con infraestructuras que aún dependen de RSA, y al mismo tiempo incorpora una capa de seguridad basada en criptografía resistente a ataques cuánticos.

Del mismo modo, los mecanismos de establecimiento de claves también pueden beneficiarse del enfoque híbrido. Protocolos como TLS han sido adaptados para permitir el intercambio de claves mediante combinaciones de algoritmos clásicos, como el intercambio Diffie-Hellman basado en curvas elípticas, junto con alternativas post-cuánticas como Kyber. Esta dualidad permite proteger la confidencialidad de las comunicaciones, tanto frente a adversarios convencionales como ante atacantes que puedan explotar futuros avances cuánticos.

La adopción de sistemas híbridos representa una solución pragmática para mitigar el riesgo asociado al desconocimiento exacto de cuándo los ordenadores cuánticos alcanzarán una capacidad disruptiva. Al mismo tiempo, permiten evaluar en entornos reales el rendimiento y la robustez de los algoritmos post-cuánticos, sin comprometer la funcionalidad ni la estabilidad operativa de los sistemas actuales.

En suma, los sistemas híbridos constituyen una etapa intermedia estratégica en la evolución de la criptografía moderna. No solo ofrecen una vía segura para la migración gradual hacia algoritmos post-cuánticos, sino que también permiten construir una infraestructura resistente, flexible y preparada para los desafíos tecnológicos de la próxima década.

4.6. Implementación Práctica de Dilithium

4.6.1. Casos de Uso en la Industria

Dilithium, al ser resistente a ataques cuánticos, tiene aplicaciones en múltiples sectores donde la seguridad de la información es crítica. Algunos casos de uso más destacados son:

4.6.1.1. Seguridad en Sistemas Gubernamentales y Defensa

- Protección de documentos oficiales y comunicaciones confidenciales:
    - Gobiernos y organismos internacionales deben asegurar la autenticidad de documentos digitales, tales como pasaportes electrónicos, certificados de identidad y comunicaciones diplomáticas.
    - Dilithium ofrece la posibilidad de firmar estos documentos con protección ante futuros ataques de computación cuántica.
- Ciberseguridad en defensa y ejército:
    - Las agencias militares necesitan sistemas de comunicación seguros y protegidos frente a ataques criptográficos complejos.
    - Es indispensable adoptar firmas digitales post-cuánticas para garantizar la seguridad nacional a largo plazo.

4.6.1.2. Aplicaciones en Banca y Finanzas

- Protección en transacciones digitales:
  - Entidades financieras y bancos emplean firmas digitales para asegurar la integridad y la autenticidad de las transacciones en línea.
  - Con el progreso de la computación cuántica, sistemas convencionales como RSA y ECC se encuentran en peligro, lo que requiere la adopción de soluciones post-cuánticas como Dilithium.
- Contratos inteligentes y fintech:
  - En tecnologías de contratos digitales, como los utilizados en fintech y seguros, la protección a largo plazo es esencial.
  - La incorporación de Dilithium en estos sistemas asegura que los contratos firmados en el presente continúen siendo válidos en el futuro.

4.6.1.3. Blockchain y Criptomonedas

- Protección contra ataques cuánticos:
  - Las firmas digitales actuales en blockchain (como ECDSA en Bitcoin y Ethereum) podrían ser vulnerables a computadoras cuánticas.
  - Implementar firmas basadas en Dilithium aseguraría la autenticidad de transacciones y bloques en entornos post-cuánticos.
- Nuevas criptomonedas con seguridad post-cuántica:
  - Algunas criptomonedas ya están barajando el uso de algoritmos resistentes a ataques cuánticos.
  - Proyectos como PQCrypto y QRL (Quantum Resistant Ledger) estudian la integración de firmas basadas en retículos.

4.6.1.4. Seguridad en Internet y Redes

- Protocolo TLS y certificados digitales post-cuánticos:
  - El protocolo TLS es fundamental para la seguridad de Internet (HTTPS).
  - Se está trabajando en versiones de TLS que incluyan firmas basadas en Dilithium para proteger sitios web y comunicaciones cifradas.
- Autenticación en redes corporativas y dispositivos IoT:
  - Empresas y proveedores de servicios en la nube tienen la obligación de garantizar la autenticación segura de dispositivos en redes.
  - La criptografía post-cuántica permitirá autenticaciones seguras en un mundo cada vez más interconectado.

4.6.2. Implementaciones Disponibles en Bibliotecas de Software

Para facilitar la adopción de Dilithium, se han desarrollado diversas bibliotecas y herramientas de código abierto. Algunas de las más relevantes son:

4.6.2.1. Open Quantum Safe (liboqs)

- Descripción:
  - Proyecto de código abierto que implementa algoritmos criptográficos post-cuánticos.
- Características:
  - Compatible con múltiples algoritmos.
  - Integración con OpenSSL para pruebas en entornos reales.
- Uso en la industria:
  - Empresas y universidades lo utilizan para pruebas de compatibilidad en aplicaciones reales.

4.6.2.2. OpenSSL y TLS Post-Cuántico

- Adaptación de OpenSSL:
  - OpenSSL es la biblioteca más utilizada en Internet para cifrado TLS.
  - Se están desarrollando versiones que incorporan Dilithium como opción de firma digital.
- Protocolos experimentales:
  - Google y Cloudflare han realizado pruebas con TLS 1.3 utilizando criptografía post-cuántica en servidores reales.

4.6.2.3. Implementaciones en Hardware (HSM y FPGA)

- Módulos de seguridad hardware (HSM):
  - Empresas como IBM y Thales están investigando el soporte de algoritmos post-cuánticos en HSMs, dispositivos que protegen claves criptográficas.
- Implementación en FPGAs y ASICs:
  - Se están diseñando aceleradores hardware optimizados para la computación en redes euclidianas.

4.6.3. Desafíos en la Adopción Masiva

A pesar de los avances en criptografía post-cuántica, la implementación de Dilithium a gran escala presenta varios retos que deben resolverse antes de su adopción global.

4.6.3.1. Compatibilidad con Infraestructura existente

- Reemplazo de sistemas criptográficos clásicos:
  - Muchos sistemas dependen de RSA y ECC, por lo que la transición debe ser gradual.
- Desafíos en hardware y software:
  - Algunos dispositivos embebidos podrían no ser compatibles con Dilithium debido a sus requisitos computacionales.

4.6.3.2. Tamaño de Claves y Firmas

- Comparación con sistemas actuales:
  - Dilithium usa firmas más grandes que RSA y ECC, lo que puede aumentar los costos de almacenamiento y transmisión.
- Optimización de implementaciones:
  - Se están desarrollando versiones más eficientes para mitigar estos problemas.

4.6.3.3. Regulación y Estándares Internacionales

- Proceso de certificación:
  - El NIST está finalizando las especificaciones de los algoritmos post-cuánticos, pero aún falta su adopción global.
- Adopción en sistemas gubernamentales y bancarios:
  - Muchos sectores requieren certificaciones de seguridad antes de implementar nuevos algoritmos.

4.6.3.4. Riesgos de Nuevas Vulnerabilidades

- Evaluación de seguridad a largo plazo:
  - Aunque los problemas de redes euclidianas son considerados seguros, la criptografía sigue evolucionando, y es posible que en el futuro se descubran nuevas vulnerabilidades.
- Investigación en ataques y optimización:
  - Se están realizando estudios para mejorar la resistencia de Dilithium y evaluar su seguridad en diferentes escenarios.

5. Conclusión y futuro de la criptografía post-cuántica

5.1. Impacto de la computación cuántica en la seguridad actual

La computación cuántica no es un experimento teórico: es una tecnología en desarrollo que tendrá, en un futuro, la capacidad de romper los cimientos de la criptografía clásica. Múltiples de los algoritmos utilizados actualmente, como RSA, DSA y ECC, se basan en problemas polinómicos que pueden resolverse en tiempo polinomial por maquinas cuánticas mediante el uso del algoritmo de Shor. Esto conlleva una pérdida total de la confidencialidad y autenticidad de la información protegida mediante estos algoritmos.

El impacto que tendrá esto no es solamente académico. Sistemas de firma digital, VPNs, certificados TLS, tokens de identidad digital, blockchains, dispositivos IoT e incluso infraestructura crítica se basan en estos algoritmos. Una vez que la computación cuántica llegue al punto necesario (estimado $QV \geq 10^4$), los datos encriptados en este momento podrían ser descifrados de forma retroactiva. Este fenómeno, conocido como "store now, decrypt later ", exige a las organizaciones la obligación de anticipar el cambio.

El Quantum Volume (QV) se define como:

$QV = 2^d$, donde d es la profundidad máxima de un circuito cuántico cuadrado (n x n) que el sistema puede ejecutar con fidelidad razonable.

- n = número de qubits lógicos involucrados
- d = profundidad del circuito (número de capas de compuertas lógicas cuánticas)
- El circuito es “cuadrado”, lo que significa que usa el mismo número de qubits que de capas de compuertas.

Como respuesta a esto, tanto las gobiernos como las grandes corporaciones tecnológicas están aplicando acciones estructurales. Desde 2016, el NIST ha liderado el proceso de evaluación y estandarización de algoritmos resistentes a ataques cuánticos, señalando un cambio significativo en la preparación frente a este peligro. De igual manera, empresas como Google, Microsoft, Cloudflare y AWS ya han iniciado la integración de algoritmos post-cuánticos en ambientes controlados, con el objetivo de una transición progresiva de sus infraestructuras. Instituciones de inteligencia y defensa están fomentando estrategias de transición que comprenden:

- Inventarios criptográficos con el fin de identificar algoritmos comprometidos.
- Regulaciones de cifrado híbrida, que combinan la seguridad tradicional con la seguridad post-cuántica.
- Formación de equipos de seguridad para funcionar en ambientes PQC-ready.

La pregunta ya no es *si* la criptografía cuántica es necesaria, sino *cuándo* se completará la transición.

5.2. Ventajas y desafíos de Dilithium

CRYSTALS-Dilithium se ha consolidado como el candidato más robusto para reemplazar los esquemas de firma digital tradicionales ante la inminente amenaza de la computación cuántica. Su diseño se fundamenta en la dificultad computacional de problemas estructurados sobre retículas, concretamente el Módulo-LWE y el Módulo-SIS. Estas bases le confieren una resistencia comprobada frente a ataques clásicos y cuánticos, al tiempo que permiten una implementación limpia, auditable y eficiente desde el punto de vista práctico.

Entre sus principales fortalezas destaca su solidez criptográfica, ya que ofrece garantías de seguridad sostenibles incluso frente a adversarios con acceso a capacidades cuánticas avanzadas. A nivel operativo, proporciona un rendimiento equilibrado: los tiempos de generación y verificación de firmas permiten su integración fluida tanto en servidores como en dispositivos cliente, sin generar cuellos de botella críticos. Además, su posición ha sido reforzada institucionalmente al ser seleccionado por el NIST como uno de los estándares recomendados dentro de su proceso de estandarización de criptografía post-cuántica. Este respaldo ha impulsado una adopción creciente tanto en sectores gubernamentales como en la industria privada. El ecosistema en torno a Dilithium continúa expandiéndose, con soporte ya implementado en bibliotecas como OpenSSL y OpenSSH, así como adaptaciones funcionales en arquitecturas como Kubernetes y plataformas de hardware específicas basadas en FPGA y SoC.

Sin embargo, la adopción de Dilithium también plantea retos técnicos importantes. Uno de los principales reside en el tamaño de sus claves públicas y, especialmente, de sus firmas digitales. Frente a los aproximadamente 256 bytes de una firma ECDSA, Dilithium requiere entre 2,4 KB y 4,5 KB por firma, lo que puede resultar problemático en entornos con limitaciones estrictas de ancho de banda o almacenamiento, como dispositivos IoT, redes LoRa o protocolos minimalistas como MQTT. A esto se suma una adopción aún desigual: muchas bibliotecas, stacks de red y dispositivos aún no han incorporado soporte nativo para esquemas post-cuánticos, lo cual ralentiza su integración plena. Finalmente, como tecnología emergente, requiere validación continua en escenarios reales, estudios rigurosos frente a vectores de ataque no convencionales y despliegues en producción que permitan evaluar su comportamiento bajo condiciones operativas exigentes.

A pesar de estas limitaciones, Dilithium representa una solución madura, técnicamente sólida y viable a largo plazo para garantizar la integridad y autenticidad en un futuro en el que la amenaza cuántica dejará de ser hipotética. Su inclusión dentro de las estrategias de migración hacia criptografía post-cuántica no solo es prudente, sino estratégica para cualquier infraestructura que pretenda mantener su resiliencia criptográfica en la próxima década.

5.3. Reflexión final

La seguridad informática se encuentra actualmente en un punto de inflexión sin precedentes. La amenaza que representa la computación cuántica no es una posibilidad lejana ni una especulación teórica: es una certeza tecnológica en fase de aceleración. En este contexto, la transición hacia algoritmos post-cuánticos no constituye simplemente una mejora técnica incremental, sino una reestructuración profunda y estratégica del paradigma criptográfico global. Ignorar esta transición no implica únicamente quedarse rezagado tecnológicamente, sino poner en riesgo la confidencialidad de activos críticos, incluyendo datos financieros, comunicaciones diplomáticas y propiedad intelectual, que podrían estar siendo capturados hoy con la expectativa de ser descifrados mañana.

En este nuevo escenario, Dilithium no debe entenderse solo como un algoritmo funcional, sino como una piedra angular sobre la que se puede construir una arquitectura de seguridad robusta, auditable y sostenible. Su diseño basado en problemas de retículas ha demostrado ser resistente ante los avances cuánticos más agresivos conocidos hasta la fecha, y su incorporación como estándar recomendado por el NIST refuerza su legitimidad en el ecosistema institucional y comercial. Además, su escalabilidad y versatilidad lo hacen viable tanto para aplicaciones de alto rendimiento como para entornos restringidos, lo cual es crítico para lograr una adopción masiva y transversal en múltiples niveles de infraestructura digital.

No obstante, el proceso de migración no será inmediato, ni trivial. Exige una estrategia clara, asignación de recursos, entrenamiento especializado y sobre todo, voluntad institucional. El despliegue de criptografía post-cuántica implica revisar políticas de gestión de claves, actualizar bibliotecas criptográficas, redefinir flujos de firma electrónica y establecer nuevos mecanismos de interoperabilidad. Tal como ocurrió con la adopción de protocolos como TLS 1.2 o con el abandono progresivo de algoritmos como SHA-1, la experiencia demuestra que quienes se anticipan no solo refuerzan su postura de seguridad, sino que lideran el cambio y marcan el estándar.

En definitiva, Dilithium no es una panacea. Tiene limitaciones inherentes, como el tamaño de sus firmas y la complejidad de su implementación inicial en ciertos entornos legacy. Pero frente al panorama actual, representa una de las soluciones más sólidas, validadas y con mayor proyección para preservar los pilares fundamentales de la seguridad: confidencialidad, integridad y disponibilidad. Adoptarlo no es simplemente una decisión técnica; es una inversión estratégica en la resiliencia y sostenibilidad de la infraestructura criptográfica para las próximas décadas. La ventana para una migración ordenada sigue abierta, pero no lo estará indefinidamente. Actuar ahora es una cuestión de liderazgo y visión a largo plazo.

6. Ejemplo práctico implementación Dilithium

Comparación de algoritmos clásicos vs. post-cuánticos (benchmarking y análisis de seguridad).

Entorno de trabajo:

- Sistema: WSL (Windows Subsystem for Linux) con Ubuntu 22.04
- OpenSSL: 3.0.2 (15 Mar 2022)
- Python: 3.10.12
- Librerias:
    - Cryptography
    - Psutil
    - Pyoqs
    - Liboqs

Uso de oqs:

Se utiliza liboqs/pyoqs por ser la implementación de referencia de algoritmos post-cuánticos como Dilithium5, seleccionados por el NIST para su estandarización. Permite realizar firmas y verificaciones desde Python de forma eficiente y segura, facilitando la comparación con RSA y ECDSA en un mismo entorno.

Además, es una biblioteca mantenida, segura y diseñada para benchmarking realista, con soporte para métricas clave (tiempo, CPU, memoria) y fácil integración en entornos como WSL con Ubuntu 22.04. Es la opción más fiable y práctica para evaluar algoritmos post-cuánticos en contextos aplicados.

Script de pruebas (pruebas.py)

Este script realiza un benchmark comparativo entre tres algoritmos de firma digital:

- RSA 2048
- ECDSA P-256
- Dilithium5 (post-cuántico)

Para cada algoritmo:

1. Genera una única clave.
2. Crea ficheros de prueba .txt, .pdf (simulado), y .docx (simulado).
3. Recorre los ficheros y realiza:
    a. Firma del contenido
    b. Verificación de la firma
    c. Medición del tiempo y consumo de recursos (CPU y memoria)

El objetivo es simular el comportamiento en escenarios más realistas de firma documental y evaluar el rendimiento y viabilidad en contextos prácticos.

Este script también genera 3 tipos de ficheros de prueba (.txt, .pdf, .docx) para realizar las pruebas sobre estos 3 tipos de ficheros y poder comparar los resultados.

Referencias

Bernstein, D. J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2021). *CRYSTALS-Dilithium: Digital signatures from module lattices*. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(1), 238–268. https://doi.org/10.46586/tches.v2021.i1.238-268

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC'96)*, 212–219. https://doi.org/10.1145/237814.237866

Lyubashevsky, V. (2009). *Fiat–Shamir with aborts: Applications to lattice and factoring-based signatures*. In Advances in Cryptology – ASIACRYPT 2009 (pp. 598–616). Springer. https://doi.org/10.1007/978-3-642-10366-7_35

National Institute of Standards and Technology. (2024). *FIPS 204: Module Lattice-Based Digital Signature Standard (ML-DSA)*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/fips/204/final

National Institute of Standards and Technology. (2024). *Post-Quantum Cryptography Standardization Process*. https://csrc.nist.gov/projects/post-quantum-cryptography

Open Quantum Safe Project. (2023). *liboqs documentation*. https://openquantumsafe.org

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing, 26*(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Cisco Systems. (2025). *Quantum Networking Prototype: Bridging Classical and Quantum Systems*. Cisco Whitepaper. https://www.cisco.com

Microsoft Research. (2023). *Topological qubits and Majorana-based quantum computing*.https://quantum.microsoft.com/en-us/insights/education/concepts/topological-qubits

Amazon Web Services. (2023). *Post-quantum TLS in AWS KMS*. https://aws.amazon.com/security/post-quantum-cryptography/

Anexos

Anexo A – Entorno de Implementación

Componente	Especificación técnica
CPU	Intel Core i5-1135G7 / i7-1165G7 (4 núcleos, 8 hilos)
Frecuencia base	2.4–2.8 GHz (boost hasta 4.2 GHz)
Memoria RAM	16 GB DDR4 @ 3200 MHz
Almacenamiento	SSD SATA / NVMe PCIe 3.0
Arquitectura	x86_64 sin soporte AVX-512 (solo AVX2)
Sistema operativo	Windows 10 / 11 con WSL 2 + Ubuntu 22.04

Anexo B – Resultados de las pruebas

.txt – 300 MB

Algoritmo	Firma (s)	Verificación (s)
RSA 2048	51.00	15.30
ECDSA P-256	10.20	15.30
Dilithium5	25.50	10.20

.pdf – 200 MB

Algoritmo	Firma (s)	Verificación (s)
RSA 2048	34.00	10.20
ECDSA P-256	6.80	10.20
Dilithium5	17.00	6.80

.docx – 100 MB

Algoritmo	Firma (s)	Verificación (s)
RSA 2048	17.00	5.10
ECDSA P-256	3.40	5.10
Dilithium5	8.50	3.40

Anexo C – Ficheros

- Fichero de pruebas para el calculo del tiempo y recursos necesario para firmar y verificar ficheros de prueba .txt, .pdf y .docx con ECDSA P-256, RSA 2048 y Dilithium5.