

# Criptografía y Blockchain

Módulo 4

# Criptografía post cuántica

# Fundamentos

La **criptografía post cuántica (PQC)** es la rama de la criptografía que **estudia algoritmos que sean resistentes al criptoanálisis cuántico**.

En 2016 NIST anunció una nueva competición para actualizar sus estándares e incluir algoritmos criptográficos post cuánticos.

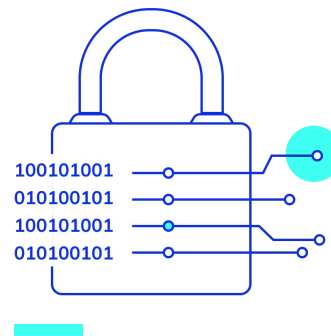
Los **nuevos estándares de criptografía de clave pública** deben incluir algoritmos adicionales de firma digital, cifrado de clave pública y establecimiento de claves.



China tiene su propio concurso abierto a través de la *Chinese Association for Cryptographic Research* (CACR) a la que se han presentado 38 candidatos.

El NIST recibió 69 algoritmos candidatos y los liberó para que los expertos los analizaran y descifrarán si pudieran. Este proceso fue abierto y transparente, y muchos de los mejores criptógrafos del mundo participaron en múltiples rondas de evaluación, lo que redujo el número de candidatos.

En julio de 2022 anunció **4 algoritmos para estandarización y cuatro candidatos para mecanismos de encapsulamiento de claves (KEM) / cifrado de clave pública.**



# Algoritmos post cuánticos estandarizados

## CRYSTALS-Kyber

Algoritmo de cifrado de clave pública y de establecimiento de clave (KEM), está cubierto en FIPS 203.

## CRYSTALS-Dilithium

Algoritmo de firma digital, está cubierto en FIPS 204.

## SPHINCS+

También diseñado para firmas digitales, está cubierto en FIPS 205.

## FALCON

También diseñado para firmas digitales, está programado para recibir su propio borrador FIPS en 2024.

## Otros algoritmos en proceso de estandarización

Todos algoritmos de cifrado de clave pública y KEM:

- BIKE
- Classic McEliece
- HQC

Las **publicaciones FIPS** proporcionan detalles que ayudarán a los usuarios a implementar los algoritmos en sus propios sistemas, como una especificación técnica completa de los algoritmos y notas para una implementación efectiva.

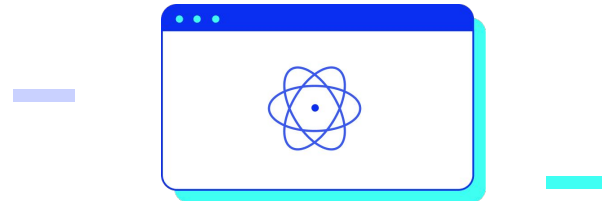
En septiembre de 2022 **NIST** lanzó una ampliación de su convocatoria para algoritmos de firma digital ya que la mayoría de los mismos se basan en el **principio de retículos estructurados (*structured lattices*)** y no hay suficiente variedad ante posibles ataques. En julio de 2023 anunció haber recibido 40 candidatos.



# Bases de los algoritmos post cuánticos

Se han propuesto varias técnicas matemáticas para construir **criptosistemas cuánticos seguros**, que incluyen funciones *hash* y pruebas simétricas de conocimiento cero, códigos de corrección de errores, retículos, ecuaciones multivariantes e isogénicas de curva elíptica supersingular.

- SPHINCS+ utiliza funciones **hash**.
- CRYSTALS-Kyber, CRYSTALS-Dilithium y FALCON utilizan **retículos**.



## Open Quantum Safe (OQS)

El proyecto [Open Quantum Safe](#) (OQS) es un proyecto de código abierto que tiene como objetivo apoyar el desarrollo y la creación de prototipos de criptografía post cuántica.

OQS consta de dos líneas principales de trabajo:

- ***liboqs***, una biblioteca en lenguaje C de código abierto, e
- **integraciones de prototipos** en protocolos y aplicaciones, incluida la biblioteca OpenSSL.

También soporta *wrappers* para C++, Go, Java, .Net, Python y Rust.



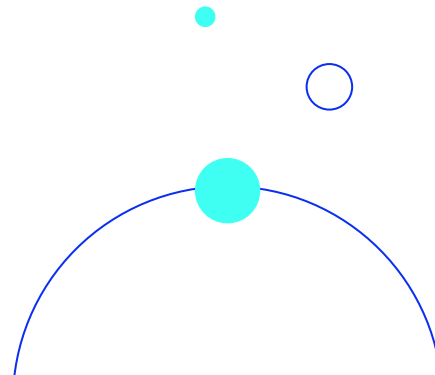


# Crystals

La **Suite criptográfica para retículos algebraicos** (*Cryptographic Suite for Algebraic Lattices: CRYSTALS*) abarca dos primitivas criptográficas:

- **Kyber**: un mecanismo de encapsulación de claves (KEM).
- **Dilithium**: un algoritmo de firma digital.

Ambos algoritmos se basan en problemas difíciles sobre **retículos modulares** y están diseñados para resistir **ataques de computadoras cuánticas**.



## Kyber

Se basa en la **dificultad de resolver el problema de aprendizaje con errores (LWE) sobre retículos modulares**. Kyber-512 apunta a una seguridad aproximadamente equivalente a AES-128, Kyber-768 a AES-192 y Kyber-1024 a AES-256. Se recomienda utilizarlo en modo híbrido en combinación con ECDH.



### Aplicaciones

- **Google** (Agosto 2023) está utilizando el algoritmo de curva elíptica X25519 con **Kyber-768** para proteger el tráfico en el navegador Chrome a partir de **Chrome 116**.
- La App **Signal** (Septiembre 2023) a pasado de **X3DH** (*Extended Triple Diffie-Hellman*) a **PQXDH** (*Post-Quantum Extended Diffie-Hellman*), que combina el protocolo de acuerdo de clave de curva elíptica X25519 con el mecanismo de encapsulación de clave post-cuántica (KEM) **CRYSTALS-Kyber**.

## Dilithium

Dilithium es un **esquema de firma digital seguro bajo ataques de mensajes elegidos basados en la dificultad de los problemas de retículos modulares**. La seguridad reside en que un adversario que tiene acceso a un oráculo de firma no puede producir una firma de un mensaje cuya firma aún no ha visto, ni producir una firma diferente de un mensaje que ya vio firmado.

Se recomienda utilizarlo en **modo híbrido** en combinación con un esquema de firma "precuántico" establecido.

Alcanza más de 128 bits de seguridad contra todos los ataques clásicos y cuánticos conocidos.

### Aplicaciones


- **Xiphera** diseña e implementa seguridad criptográfica probada para sistemas integrados. Ofrece núcleos criptográficos de propiedad intelectual (IP) seguros y altamente optimizados para FPGA y ASIC. Su familia **xQlave®** incluye mecanismos de encapsulación de claves de seguridad cuántica y un esquema de firma digital basados en **Crystals Kyber** y **Crystals Dilithium** respectivamente.
- **Castle Shield Holdings, LLC** utiliza **Crystals Kyber** y **Crystals Dilithium** para su producto Aeolus VPN.

## QKD, QC y PQC

Algunas organizaciones han recomendado el uso de criptografía **post cuántica (PQC)** como alternativa a la distribución de **claves cuánticas (QKD)** debido a los problemas que plantea en el uso práctico, entre ellas la Agencia de Seguridad Nacional de EE.UU. (NSA), la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Centro Nacional de Ciberseguridad del Reino Unido (NCSC) y la Secretaría Francesa de Defensa y Seguridad (ANSSI).

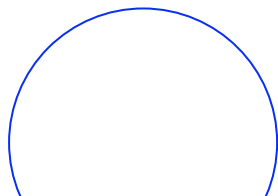
Las teorías publicadas sugieren que la física permite que **QKD o QC detecten la presencia de un espía, una característica no proporcionada en la criptografía estándar.**

Los problemas que vislumbran estas organizaciones se pueden resumir en los puntos que se muestran en los *slides* siguientes.



- a. **QKD es solo una solución parcial:** no proporciona un medio para autenticar la fuente de transmisión. Por lo tanto, la autenticación de origen requiere el uso de criptografía asimétrica o claves previas. Además, los servicios de confidencialidad que ofrece QKD pueden proporcionarse mediante PQC, que suele ser menos costosa con un perfil de riesgo mejor entendido.
- b. **QKD aumenta los costos de infraestructura y los riesgos de amenazas internas:** las redes QKD con frecuencia requieren el uso de relés confiables, lo que implica un costo adicional para las instalaciones seguras y un riesgo de seguridad adicional de las amenazas internas.
- c. **QKD requiere equipos de propósito especial:** QKD se basa en propiedades físicas, y su seguridad se deriva de comunicaciones únicas de capa física. Esto requiere que los usuarios alquilen conexiones de fibra dedicadas o administren físicamente transmisores de espacio libre. No se puede implementar en *software* o como un servicio en una red, y no se puede integrar fácilmente en equipos de red existentes. Dado que QKD está basado en *hardware*, también carece de flexibilidad para actualizaciones o parches de seguridad.

d. **QKD aumenta el riesgo de denegación de servicio:** la sensibilidad a un espía como base teórica para las reclamaciones de seguridad de QKD también muestra que la denegación de servicio es un riesgo significativo.



e. **Asegurar y validar la QKD es un desafío importante:** la seguridad real proporcionada por un sistema QKD no es la seguridad incondicional de las leyes de la física (como se modela y a menudo se sugiere), sino más bien la seguridad más limitada que se puede lograr mediante diseños de *hardware* e ingeniería. Sin embargo, la tolerancia al error en la seguridad criptográfica es muchos órdenes de magnitud menor que en la mayoría de los escenarios de ingeniería física, lo que hace que sea muy difícil de validar. El *hardware* específico utilizado para realizar QKD puede introducir vulnerabilidades, lo que resulta en varios ataques bien publicitados en sistemas QKD comerciales.

**¡Sigamos  
trabajando!**