



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Hacia protocolos de comunicaciones IP resistentes a la computación cuántica

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Daniel Porras Sánchez
DIRECTOR: Miguel Rodelgo Lacruz
CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Hacia protocolos de comunicaciones IP
resistentes a la computación cuántica*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

UniversidadeVigo

RESUMEN

La seguridad de las comunicaciones en Internet es esencial para proteger datos sensibles y garantizar la privacidad en un mundo cada vez más conectado. La computación cuántica plantea una amenaza significativa para los protocolos criptográficos actuales, al comprometer los algoritmos de clave pública que utilizan.

Este trabajo aborda esta problemática evaluando soluciones de resistencia cuántica y su integración en infraestructuras y protocolos existentes. Aunque la construcción de un ordenador cuántico criptográficamente relevante es improbable en la próxima década, el riesgo de ataques 'cosecha-ahora-descifra-después', donde se almacenan datos cifrados hoy para vulnerarlos con futuras capacidades cuánticas, subraya la urgencia de implementar soluciones que protejan la confidencialidad a largo plazo.

Entre las soluciones para dotar de resistencia cuántica a los protocolos destacan la distribución cuántica de claves y la criptografía post-cuántica. La primera ofrece seguridad teórica incondicional basada en principios cuánticos, pero enfrenta limitaciones tecnológicas y económicas que restringen su uso. Por otro lado, la criptografía post-cuántica utiliza matemáticas resistentes a ataques cuánticos, sin requerir tecnologías cuánticas, por lo que resulta compatible con las infraestructuras actuales.

La adopción de enfoques híbridos en los protocolos, combinando algoritmos clásicos y post-cuánticos, es una solución flexible y conservadora para iniciar la transición hacia sistemas con resistencia cuántica. Esta estrategia mitiga el riesgo de ataques 'cosecha-ahora-descifra-después' y ofrece un margen de seguridad ante posibles vulnerabilidades en los algoritmos post-cuánticos, sentando una base sólida para la evolución de los protocolos hacia la resistencia cuántica.

PALABRAS CLAVE

Criptografía, Seguridad, Protocolo, Cuántica, Post-cuántica.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción.....	5
1.1 Resumen ejecutivo	6
2 Seguridad en comunicaciones IP	8
2.1 Seguridad de la información	8
2.2 Criptografía simétrica y de clave pública	11
2.3 Seguridad de las primitivas criptográficas	15
2.4 Arquitectura de protocolos criptográficos.....	17
2.5 Autenticación y establecimiento de clave (fase 1).....	19
2.6 Intercambio de datos cifrados y autenticados (fase 2)	21
3 Amenaza y resistencia cuánticas	24
3.1 La amenaza cuántica a los criptosistemas.....	24
3.2 Computación multidimensional y algoritmos cuánticos.....	25
3.3 El algoritmo de factorización de Shor.....	28
3.4 El algoritmo de búsqueda de Grover.....	30
3.5 Hitos y desafíos de la computación cuántica	31
3.6 El camino hacia la factorización cuántica.....	34
3.7 Resistencia frente a la amenaza cuántica	36
4 Comunicaciones cuánticas	39
4.1 Distribución cuántica de claves.....	39
4.2 Distribución cuántica de claves discreta	41
4.3 Limitaciones de la distribución cuántica de claves.....	43
4.4 Seguridad de la distribución cuántica de claves.....	44
4.5 De la distribución de claves al Internet cuántico	46
4.6 Redes de distribución cuántica de claves	49
4.7 Controversia sobre la idoneidad de QKD para resistencia cuántica	51
5 Criptografía post-cuántica	53
5.1 Criptografía (de clave pública) post-cuántica	53
5.2 Proceso de estandarización del NIST.....	55
5.3 Fundamentos matemáticos en criptografía post-cuántica	57
5.4 Seguridad de los algoritmos post-cuánticos.....	61

5.5 Transición a firmas digitales post-cuánticas	63
5.6 Transición a encapsulamientos de clave post-cuánticos	65
6 Resistencia cuántica en protocolos IP	68
6.1 Amenaza cuántica a los protocolos criptográficos.....	68
6.2 Resistencia cuántica con criptografía simétrica	69
6.3 Resistencia cuántica con comunicaciones cuánticas.....	71
6.4 Resistencia cuántica con criptografía post-cuántica	73
7 Conclusiones	80
8 Bibliografía.....	83
9 Acrónimos	98

ÍNDICE DE FIGURAS

Figura 1-1 Estructura del trabajo y objetivos	5
Figura 2-1 Representación de las capas del modelo TCP/IP [5]	9
Figura 2-2 Cifrado con algoritmo asimétrico [29]	12
Figura 2-3 Intercambio de clave Diffie Hellman [30]	13
Figura 2-4 Firma digital con algoritmo asimétrico [34]	14
Figura 2-5 Fases de un protocolo criptográfico	17
Figura 2-6 Sesiones sucesivas de un protocolo criptográfico	18
Figura 3-1 Ordenador cuántico de IBM en 2021 [69]	25
Figura 3-2 Representación gráfica de un qubit y sus propiedades [70]	26
Figura 3-3 Hoja de ruta de Google hacia el ordenador cuántico [99]	32
Figura 3-4 Hoja de ruta de IBM hacia el ordenador cuántico [104]	33
Figura 3-5 Estimación de expertos sobre la probabilidad de factorizar RSA-2048 [66]	35
Figura 3-6 Ventana de oportunidad para el ataque 'cosecha-ahora-descifra-después' [66]	36
Figura 4-1 Esquema del protocolo BB84 para DV-QKD [135]	41
Figura 4-2 Pérdidas típicas por atenuación en enlaces de fibra óptica y de espacio libre [144]	44
Figura 4-3 Comunicaciones a escala global combinando QKD terrestre y satelital [144]	48
Figura 4-4 Distribución hop-by-hop de una clave empleando dos nodos intermedios [170]	49
Figura 4-5 Arquitectura en capas de una red QKD [170]	50
Figura 5-1 Diagramas de los esquemas PKE y KEM [184] [185]	55
Figura 5-2 Familias de algoritmos PQC según su fundamento matemático	58
Figura 6-1 Arquitectura de red (izquierda) y acuerdo de clave (derecha) en SKIP [256]	72
Figura 6-2 Compartición de secretos en IPSEC usando DH y KEM [273]	75
Figura 6-3 Derivación de claves de sesión en TLSv1.3 híbrido [274]	77
Figura 6-4 Acuerdo del secreto compartido en TLSv1.3 híbrido [279]	78

ÍNDICE DE TABLAS

Tabla 2-1. Esquemas de cifrado autenticado soportados por protocolos criptográficos	23
Tabla 3-1. Crecimiento de las complejidades de GNFS y Shor	28
Tabla 3-2. Implementaciones del algoritmo de Shor.....	29
Tabla 3-3. Implementaciones del algoritmo de Grover.....	31
Tabla 5-1. Algoritmos PQC en las fases finales del concurso del NIST [190]	56
Tabla 5-2. Niveles de seguridad para los algoritmos PQC definidos por NIST [189]	57
Tabla 5-3. Longitudes de clave y firma de algunos algoritmos de firma digital [243] [244]	63
Tabla 5-4. Tiempo de ejecución de algunos algoritmos PQC de firma digital [244]	64
Tabla 5-5. Longitudes de clave y cifrado de algoritmos KEM (según especificaciones).	66
Tabla 5-6. Tiempo de ejecución de algunos algoritmos KEM [252]	66

1 INTRODUCCIÓN

En un mundo cada vez más interconectado, Internet se ha convertido en un pilar fundamental de la sociedad moderna. Su infraestructura sostiene no solo actividades cotidianas como la comunicación personal y el comercio digital, sino también sistemas críticos para la economía, la salud pública, la educación y la defensa. La omnipresencia de las redes digitales ha transformado las raíces de la sociedad moderna, pero también ha generado un panorama complejo de amenazas que comprometen la seguridad de la información que se transmite por Internet.

La seguridad de las comunicaciones en Internet depende de un delicado equilibrio entre la sofisticación de los ataques cibernéticos y las tecnologías disponibles para proteger la información. En este sentido, la criptografía moderna desempeña un papel fundamental, proporcionando las bases para protocolos que garantizan la privacidad de los datos, la autenticación de usuarios y la protección contra modificaciones maliciosas. Sin embargo, la seguridad de estos protocolos se enfrenta a un gran desafío: el desarrollo de la computación cuántica, una tecnología que amenaza con debilitar la seguridad de las bases matemáticas que fundamentan los sistemas criptográficos actuales.

La computación cuántica introduce un nuevo paradigma en la resolución de problemas computacionales basado en fenómenos de la física cuántica. Se han desarrollado algoritmos cuánticos que, en teoría, son capaces de reducir significativamente el margen de seguridad de los algoritmos criptográficos usados en la actualidad, especialmente de los de clave pública. Aunque aún no existe un ordenador cuántico capaz de ejecutar estos algoritmos, los avances recientes de la computación cuántica sugieren que la tecnología es viable y que su construcción es solo cuestión de tiempo. Este futurible ordenador cuántico avanzado sería capaz de comprometer la seguridad de muchos de los protocolos criptográficos utilizados en la actualidad y poner en riesgo la información que transita por Internet.

Ante este escenario, es crucial avanzar hacia algoritmos y protocolos criptográficos que resistan tanto los desafíos actuales de seguridad en Internet como las amenazas cuánticas futuras. La transición hacia criptosistemas resistentes a un ordenador cuántico con la capacidad de comprometer algoritmos criptográficos será compleja y requerirá tiempo para garantizar una implementación efectiva y segura, por lo que es fundamental actuar con antelación. El presente trabajo tiene como objetivos describir la amenaza cuántica y evaluar su impacto en algoritmos y protocolos criptográficos, presentar diferentes soluciones que permiten dotar a los protocolos de resistencia cuántica, principalmente la criptografía cuántica y la post-cuántica, y analizar cómo se están integrando las técnicas de resistencia cuántica en los protocolos de comunicaciones IP, así como los desafíos de esta integración.

La Figura 1-1 representa la estructura del trabajo:



Figura 1-1 Estructura del trabajo y objetivos

1.1 Resumen ejecutivo

Antes de abordar los objetivos, se establece un **marco teórico sobre criptografía moderna y su empleo en protocolos IP** para garantizar los servicios de confidencialidad, integridad, autenticación y no repudio en comunicaciones de Internet (sección 2). Este marco es fundamental para analizar las soluciones destinadas a dotar de resistencia cuántica a los protocolos de comunicaciones. Se describen la criptografía simétrica y la de clave pública, y se explica el concepto de protocolo criptográfico y su arquitectura general, con una fase inicial en la que las partes se autentican y establecen un secreto compartido, seguida de otra fase en la que intercambian datos cifrados y autenticados con claves derivadas de dicho secreto. Además, se analizan propiedades clave y particularidades de esta arquitectura, ilustradas con ejemplos de protocolos criptográficos ampliamente utilizados en Internet.

En la sección 3 se aborda el primer objetivo del trabajo: describir y evaluar la **amenaza que representa el desarrollo de la computación cuántica para los algoritmos y protocolos criptográficos actuales**. Se describen los fundamentos de la computación cuántica y los algoritmos cuánticos más relevantes desde el punto de vista criptográfico, capaces de reducir el margen de seguridad de los algoritmos clásicos utilizados en los protocolos IP. Además, se analiza el estado actual de la computación cuántica y se exponen los retos que ha de superar para alcanzar un ordenador cuántico capaz de ejecutar dichos algoritmos, así como una prospectiva del tiempo estimado para su posible construcción. También se señala la amenaza que supone que actores maliciosos almacenen comunicaciones actuales para descifrarlas en el futuro mediante esta tecnología. Finalmente, se subraya la necesidad de comenzar urgentemente la transición hacia protocolos resistentes a esta amenaza, que se espera sea un proceso complejo y prolongado.

El segundo objetivo del trabajo consiste en analizar las principales **alternativas de resistencia cuántica: la criptografía cuántica, especialmente la distribución cuántica de claves, y la criptografía post-cuántica**. En las secciones 4 y 5, respectivamente, se analizan estas tecnologías y se evalúan aspectos como su viabilidad, aplicabilidad, limitaciones y grado de madurez. Se explica que, mientras que la criptografía cuántica aprovecha fenómenos cuánticos para evitar los algoritmos de clave pública amenazados, la criptografía post-cuántica introduce un conjunto de algoritmos de clave pública cuya seguridad computacional se basa en problemas matemáticos distintos a los que sustentan los algoritmos clásicos y que, en teoría, resultarán inabordables incluso para los ordenadores cuánticos.

En la sección 4 se describe la distribución cuántica de claves, un método que permite a dos partes acordar una clave mediante un canal cuántico. Aunque su seguridad es incondicional desde un punto de vista teórico, esta tecnología presenta importantes limitaciones, como la limitada distancia de transmisión y la baja tasa de generación de claves, causadas por la atenuación de la señal fotónica. Además, requiere equipos específicos que son complejos, costosos y, en ocasiones, susceptibles a ataques de canal lateral. Se expone cómo estas limitaciones, junto con cierta inmadurez de la tecnología, como la falta de repetidores cuánticos, dificultan su adopción masiva como reemplazo de la infraestructura actual de Internet y que su aplicación queda limitada a día de hoy a redes terrestres de alcance restringido y demostradores satelitales.

Se describe en la sección 5 que los algoritmos post-cuánticos evitan usar las bases matemáticas susceptibles de compromiso cuántico, garantizando así una resistencia cuántica sin necesidad de equipamiento específico. Esto permite, a priori, aprovechar las infraestructuras de comunicación actuales para la transición hacia protocolos resistentes a la amenaza cuántica. Se analizan los fundamentos matemáticos alternativos, junto con sus ventajas y desventajas, los principales algoritmos de firma digital y encapsulamiento de clave de cada tipo, y los primeros estándares disponibles. Su empleo no está, no obstante, exento de dificultades.

Los algoritmos post-cuánticos son más complejos que los clásicos, lo que dificulta garantizar su seguridad tanto desde una perspectiva teórica como en su implementación práctica; de hecho, varios esquemas post-cuánticos desarrollados en los últimos años han sido comprometidos. Además, se detalla cómo estos algoritmos suelen ser más costosos en términos de longitud de claves, cifrados y firmas, así como en rendimiento.

Para finalizar, en la sección 6 se aborda el último de los objetivos del trabajo, que consiste en analizar las **soluciones en desarrollo para dotar de resistencia cuántica a los protocolos criptográficos utilizados en las comunicaciones IP**, de acuerdo con lo presentado en las secciones anteriores. Se argumenta que el enfoque de la transición se centra en la autenticación de las partes y el establecimiento de la clave de sesión en los protocolos, dado que la resistencia de la criptografía simétrica con una longitud de clave suficiente garantiza un intercambio seguro de datos cifrados y autenticados. Asimismo, se señala que se está dedicando un esfuerzo significativamente mayor al establecimiento de claves que a la autenticación, con el fin de proteger cuanto antes la confidencialidad de las comunicaciones frente a adversarios capaces de almacenarlas para su futura explotación con un ordenador cuántico.

Se exploran los avances en curso para dotar de resistencia cuántica a las comunicaciones IP, con los tres principales enfoques: criptografía simétrica, comunicaciones cuánticas y criptografía post-cuántica. En cada caso, se presentan las ventajas de su aplicación, las limitaciones relacionadas con su adopción y la compatibilidad con el Internet actual. Se argumenta que la criptografía post-cuántica representa la solución más apropiada para aprovechar la infraestructura existente y que la apuesta mayoritaria se centra en la hibridación de algoritmos clásicos y post-cuánticos con el fin de minimizar los riesgos de seguridad que supone sustituir algoritmos maduros por otros más recientes aún bajo el escrutinio de la comunidad científica. Además, se detallan ejemplos prácticos de adaptación en protocolos criptográficos ampliamente utilizados, mostrando cómo se están modificando para integrar estas aproximaciones y garantizar su seguridad frente a adversarios clásicos y cuánticos.

2 SEGURIDAD EN COMUNICACIONES IP

En esta sección se introducen los conceptos básicos de seguridad de la información de confidencialidad, integridad, la autenticación y no repudio, que resultan fundamentales para garantizar la seguridad de las comunicaciones en una red abierta e insegura como es Internet, y se explica cómo la criptografía proporciona técnicas efectivas para implementar estos servicios. Se describe la criptografía simétrica y la de clave pública, exponiendo cómo esta última, además de cifrar, permite firmar digitalmente e intercambiar secretos de forma segura.

También se aborda en la sección la seguridad de las primitivas criptográficas frente a adversarios, tanto pasivos como activos, que pueden llegar a vulnerar estas primitivas y comprometer alguno de los servicios de seguridad que proporcionan. Se exponen los diferentes roles que pueden tener los adversarios y diferentes nociones de seguridad teórica para los esquemas criptográficos, desde la seguridad incondicional ideal hasta la seguridad computacional en la que se fundamentan los algoritmos simétricos y asimétricos que se utilizan en la actualidad.

Además, se introduce el concepto de protocolo criptográfico, pilar fundamental en la seguridad de las comunicaciones modernas. Existen cientos de protocolos criptográficos utilizados en las diferentes capas del modelo TCP/IP para garantizar la seguridad de la información que se transmite por Internet, en función de las necesidades de los usuarios en red. Se describe la arquitectura general de estos protocolos en dos fases, una de autenticación y establecimiento de clave de sesión y otra la que se intercambian los datos cifrados y autenticados con claves derivadas de la clave de sesión.

Finalmente, se profundiza en cada una de las dos fases de esta arquitectura de protocolo criptográfico. Se definen conceptos importantes como la frescura de las claves de sesión, el secreto hacia adelante, la autenticación basada en secretos pre-compartidos o en terceras partes de confianza, la diferencia entre el transporte y el acuerdo de claves, los códigos de autenticación de mensajes, etc. Aunque esta arquitectura es de uso general, cada protocolo tiene sus particularidades, algunas de las cuales se ejemplifican con protocolos de uso extendido como IPSEC o TLS.

2.1 Seguridad de la información

Hoy en día vivimos en una sociedad altamente digitalizada e interconectada donde la mayoría de nuestras actividades cotidianas, desde las finanzas hasta la comunicación y la gestión de servicios esenciales, se realizan en línea. A medida que aumenta nuestra dependencia de Internet y de las tecnologías digitales, también crecen las amenazas y riesgos asociados al manejo de datos, lo que hace fundamental garantizar su **seguridad**. La información se ha convertido en un activo muy valioso para personas, empresas y gobiernos, y el acceso a la misma o su alteración no autorizados puede acarrear graves consecuencias.

Para garantizar la seguridad de la información es necesario abordar diferentes aspectos como la confidencialidad, la integridad de los datos, la autenticación tanto de entidades como del origen de los datos y el no repudio. La **criptografía** juega un papel fundamental en este sentido, ya que proporciona técnicas efectivas para implementar todos estos servicios [1]:

- La **confidencialidad** (o privacidad) es un servicio cuyo objeto es proteger el contenido de la información de todos, excepto de aquellos autorizados para acceder a ella.
- La **integridad de los datos** es un servicio que proporciona la capacidad de detectar la manipulación no autorizada de la información (inserción, eliminación o sustitución de datos).
- La **autenticación** es un servicio relacionado con la identificación, aplicable tanto a entidades (los comunicantes deben identificarse mutuamente) como a la propia información (el origen de los datos debe estar asegurado).

- El **no repudio** es un servicio que impide que una entidad niegue compromisos o acciones realizadas con anterioridad, y resulta fundamental para la resolución de conflictos.

Estos cuatro servicios son fundamentales tanto para garantizar la seguridad tanto de los datos en reposo (almacenados) como de los datos en tránsito (transmitidos), aunque las técnicas criptográficas empleadas y su implementación difieren en ambos casos. A lo largo de este trabajo se pondrá el foco en la seguridad de los datos que se transmiten por **Internet**, una red abierta que expone dichos datos a multitud de amenazas y actores maliciosos.

En este contexto, existen protocolos de comunicaciones que integran técnicas criptográficas robustas para garantizar la confidencialidad e integridad de los datos, la autenticación y el no repudio, denominados **protocolos criptográficos**. Estos protocolos se utilizan a diario por miles de millones de personas en todo el mundo, por lo que su diseño e implementaciones son fundamentales para conseguir la seguridad de la información que se transmite por Internet [1] [2] [3]. Una forma habitual de clasificar los protocolos es de acuerdo a las capas del modelo TCP/IP, representado en la Figura 2-1, ya que facilita su análisis y comprensión en este contexto [4].

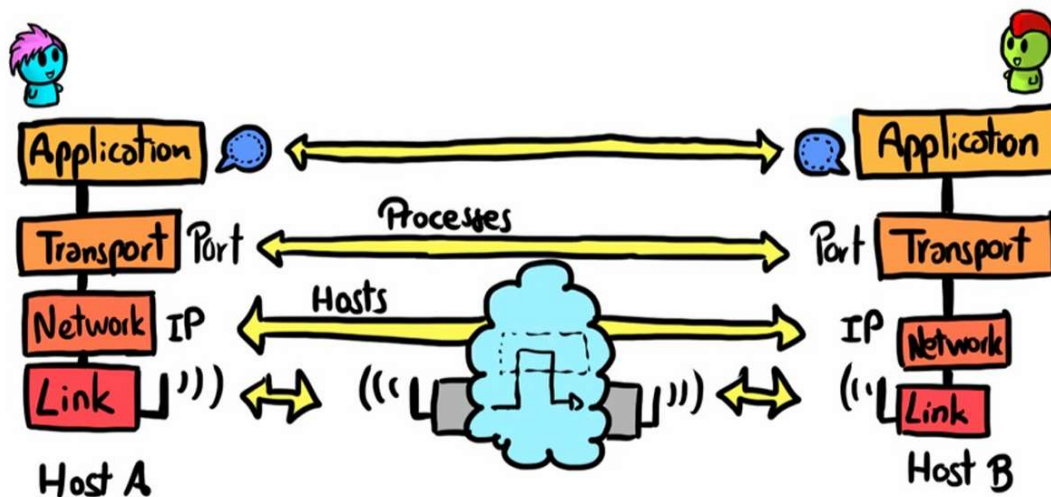


Figura 2-1 Representación de las capas del modelo TCP/IP [5]

En la **capa de enlace** se distinguen protocolos criptográficos como MACSEC [6], para conexiones Ethernet, y protocolos inalámbricos como WPA (*Wi-Fi Protected Access*), con versiones WPA2 [7] y WPA3 [8], el propio de Bluetooth [9] y ZIGBEE [10]. En la **capa de red**, el estándar es IPSEC (*Internet Protocol Security*), aunque hay otros relevantes como los propios de las aplicaciones OPENVPN [11] o WIREGUARD [12]; este tipo de protocolos se utiliza habitualmente para desplegar redes privadas virtuales o túneles cifrados en conexiones punto a punto. El protocolo IPSEC está compuesto por varios componentes, aunque típicamente se implementa como una combinación de IKE (*Internet Key Exchange*), en sus versiones IKEv1 [13] e IKEv2 [14], y ESP (*Encapsulating Security Payload*) [15].

En la **capa de transporte**, el protocolo más utilizado es TLS (*Transport Layer Security*) en sus diferentes versiones, así como sus variantes DTLS (*Datagram Transport Layer Security*) [16] y QUIC (*Quick UDP Internet Connections*) [17]. TLS presenta diferencias notables entre sus versiones, particularmente en la transición de TLSv1.2 [18] a TLSv1.3 [19]. Por último, en la **capa de aplicación** hay una gran variedad de protocolos para proporcionar seguridad a la comunicación entre aplicaciones, adaptándose a diferentes necesidades. Ejemplos representativos son: SSH (*Secure Shell*) [20], muy utilizado para conexión remota a servidores; S/MIME (*Secure/Multipurpose Internet Mail Extensions*) [21], estándar de correo electrónico seguro basado en PGP (*Pretty Good Privacy*) [22] [23]; y SIGNAL, protocolo de mensajería instantánea que implementa cifrado de extremo a extremo para garantizar la confidencialidad de los mensajes frente a los servidores que proporcionan el servicio.

A lo largo de los años, se han identificado muchos tipos de ataque dirigidos tanto a las primitivas criptográficas como a los propios protocolos, que se pueden categorizar en dos tipos: pasivos y activos. Un **ataque pasivo** es aquel en el que el adversario es capaz de monitorizar el canal de comunicación, con el objetivo de recopilar información, pero no puede modificar los mensajes que se intercambian por el canal [1] [3]. Aunque no altera directamente los datos, un atacante pasivo puede comprometer la confidencialidad de los datos si estos no están cifrados adecuadamente. Hay dos tipos de ataque pasivo: el **COA** (*Ciphertext Only Attack*), en el que el adversario intenta deducir mensajes o claves a partir de los cifrados que observa en el canal, y el **KPA** (*Known Plaintext Attack*), una mejora del anterior en la que el adversario conoce además algunos mensajes asociados a los cifrados observados.

En contraste, en un **ataque activo** el adversario puede no solo observar el canal, sino también intervenir directamente en el mismo y llegar a modificar, eliminar, insertar o reordenar los mensajes que se transmiten, poniendo en riesgo no solo la confidencialidad, sino también la integridad y la autenticidad de los datos [1] [3]. Los ataques activos pueden estar directamente dirigidos a alguna primitiva criptográfica, aunque lo más habitual es que se dirijan contra los protocolos que las integran e implementan, con independencia de la seguridad de las propias primitivas criptográficas sobre las que se construyen.

Este tipo de ataques representa, por lo tanto, una amenaza más grave para la seguridad que los ataques pasivos. Es habitual clasificar los ataques activos en función del grado de control del adversario sobre las partes involucradas o sobre el canal de comunicación, distinguiendo tres categorías: ataques en los que el adversario compromete una de las partes, ataques en los que interactúa con ellas para explotar vulnerabilidades y ataques en los que se suplanta la identidad de alguna de las partes.

Son especialmente peligrosos los ataques en los que el adversario puede **acceder a una de las partes** involucradas en la comunicación, bien alterando el funcionamiento de los dispositivos y los algoritmos que implementan o bien extrayendo información sensible, ya que estos pueden tener éxito incluso ante protocolos y algoritmos criptográficos robustos. Entre estos ataques destacan los ataques mediante **malware**, en los que el adversario introduce *software* malicioso con el objetivo de capturar, por ejemplo, las contraseñas introducidas por el usuario legítimo o sustraer archivos que almacenen claves. También los ataques de **canal lateral**, capaces de inferir claves a partir de información derivada de la implementación de algoritmos criptográficos, como el tiempo de ejecución, el consumo de energía o las emisiones electromagnéticas.

En otras ocasiones el adversario es capaz de **interactuar directamente con las partes** para explotar vulnerabilidades en los algoritmos o los protocolos. Cabe destacar en esta categoría los ataques contra la confidencialidad de algoritmos criptográficos en los que el adversario no solo intercepta, como en COA y KPA, sino que además es capaz de obtener el cifrado de mensajes de su elección (**CPA**, *Chosen-plaintext Attack*), o seleccionar cifrados específicos y obtener sus correspondientes descifrados (**CCA**, *Chosen-ciphertext Attack*), deduciendo a partir de estas interacciones información útil para recuperar los mensajes transmitidos a partir de sus cifrados. En las versiones adaptativas de estos ataques, **CPA2** y **CCA2**, el adversario puede basar su elección de mensajes o cifrados en las respuestas obtenidas en peticiones previas, aumentando así la eficacia del ataque.

A esta misma categoría de interacción directa pertenecen muchos de los ataques habituales a protocolos criptográficos. Algunos explotan su carácter iterativo y la posibilidad de interactuar de manera repetida con las partes, como por ejemplo el ataque de **downgrade**, en el cual el adversario manipula la negociación inicial de un protocolo para forzar a las partes a utilizar versiones antiguas y menos seguras del mismo. Otro ataque de esta categoría es el de **repetición**, que se basa en la retransmisión de mensajes legítimos previamente interceptados; en este caso el adversario no necesita interactuar activamente con el protocolo, sino que simplemente reutiliza mensajes válidos en un contexto incorrecto para inducir un comportamiento anómalo en el protocolo que pueda explotar.

La última categoría de ataque activo corresponde a aquellos en los que el adversario es capaz de **suplantar la identidad de una o varias partes** legítimas, engañando así a los participantes en la comunicación para modificar o redirigir los mensajes, lo que permite vulnerar la confidencialidad, integridad y autenticidad de los datos que se transmiten. Este tipo de ataque se denomina de **hombre en el medio**, MITM por sus siglas en inglés, cuando la comunicación tiene lugar entre dos partes y el adversario es capaz de engañar a ambas haciéndose pasar por cada una de ellas ante la otra. Además del MITM, existen otros ataques de suplantación de identidad, como el de **suplantación de servidor** en arquitecturas cliente-servidor, en el que el adversario crea un servidor falso imitando a uno legítimo para engañar a los clientes.

A continuación, se describen las herramientas criptográficas que utilizan los protocolos de las diferentes capas de Internet para garantizar los servicios de seguridad descritos y evitar ataques pasivos y activos, así como la estructura general de los protocolos basados en estas herramientas.

2.2 Criptografía simétrica y de clave pública

Tal y como relata Kahn en *The Codebreakers* [25], la criptografía lleva usándose desde las civilizaciones antiguas como herramienta para proteger secretos, fundamentalmente en los ámbitos militar y diplomático, y en este sentido alcanzó su auge en el siglo XX, cuando desempeñó un papel fundamental en el devenir de las guerras mundiales. Hasta la proliferación de los sistemas informáticos y de comunicaciones en la década de 1960, la criptografía empleada era exclusivamente **simétrica**, es decir, se empleaban algoritmos de cifrado y descifrado que usan una misma clave para operar.

Si bien este tipo de criptografía resultaba efectivo en escenarios controlados, donde las partes podían acordar y proteger la clave compartida de forma segura, no cubría las nuevas necesidades que planteaban la información en formato digital y su intercambio por redes de comunicación abiertas. En la década de 1970, el trabajo de Feistel en IBM culminó con la estandarización del algoritmo de cifrado simétrico **DES** (*Data Encryption Standard*) para protección de información no clasificada en EEUU [26]. Sin embargo, la criptografía simétrica se enfrentaba a dos problemas fundamentales: la dificultad para compartir claves de forma segura en redes abiertas y los problemas para gestionar dichas claves cuando crecía el número de usuarios.

Fue entonces cuando se desarrolló la **criptografía de clave pública** (o asimétrica), concepto que introdujeron Diffie y Hellman en su artículo de 1976 “*New Directions in Cryptography*” [27], trabajo en el que definieron un método para intercambio de claves en una red abierta cuya seguridad se basa en la dificultad del problema del logaritmo discreto, que hoy día es conocido como intercambio **DH**. Poco después, en 1978, Rivest, Shamir y Adleman del MIT definieron el primer esquema de cifrado con clave pública “*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*” [28], cuya seguridad depende de la dificultad de factorizar números enteros grandes. Este esquema, que se conoce actualmente como **RSA**, no solo permitía cifrar información, sino también firmarla digitalmente.

Mientras que los algoritmos de cifrado simétrico utilizan la misma clave para cifrar y descifrar, en los algoritmos de cifrado de clave pública **cada usuario tiene un par de claves** relacionadas entre sí, la clave pública K_{pub} y la privada K_{pri} . Estas claves verifican que K_{pub} puede derivarse sencillamente a partir de K_{pri} , pero que la tarea de calcular K_{pri} a partir de K_{pub} es computacionalmente inabordable, de manera que los usuarios de una red pueden publicar sus K_{pub} sin revelar las K_{pri} asociadas. Tal y como se representa gráficamente en la Figura 2-2, el emisor emplea la clave pública del receptor para cifrar el mensaje y proteger su confidencialidad, mensaje cifrado que solo el receptor puede descifrar con la clave privada correspondiente.

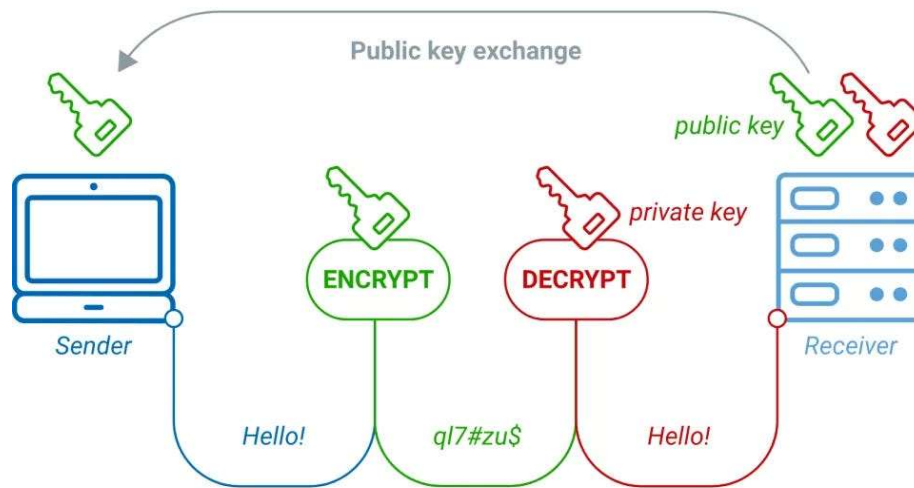


Figura 2-2 Cifrado con algoritmo asimétrico [29]

Más formalmente, un esquema de cifrado con clave pública, conocido típicamente como **PKE** por sus siglas en inglés, está compuesto por una terna de funciones Gen, Encrypt y Decrypt. La primera función $(K_{\text{pri}}, K_{\text{pub}}) = \text{Gen}(s)$ genera un par de claves privada K_{pri} y pública K_{pub} para el algoritmo, de acuerdo al nivel de seguridad s que se pretenda alcanzar; es habitual que este nivel de seguridad se defina en función de la longitud de clave. La función $c = \text{Encrypt}(K_{\text{pub}}, m)$ cifra un mensaje m con la clave K_{pub} y la función $m = \text{Decrypt}(K_{\text{pri}}, c)$ descifra el cifrado c con la clave K_{pri} para recuperar el mensaje original m , pudiendo devolver en ocasiones $\perp$ en caso de error.

Gracias a la dualidad de claves, la criptografía de clave pública es **más escalable** que la simétrica. Como se ha explicado, cada comunicante publica o comparte su K_{pub} y permite que cualquiera (incluso actores maliciosos) pueda cifrar un mensaje para él con esta clave, mensaje que solo el legítimo destinatario podrá descifrar con la correspondiente K_{pri} . Así pues, en una red de N usuarios que emplean cifrado asimétrico el número de claves crece proporcionalmente a N , mientras que con cifrado simétrico crece proporcionalmente a $N \cdot (N - 1) / 2$ dado que cada usuario ha de compartir una clave con todos los demás [1] [27] [28].

La criptografía de clave pública también se utiliza para el intercambio de claves confidencial entre dos partes, lo que se conoce como **intercambio DH** [27]. Este protocolo permite que las partes intercambien una clave secreta común a través de un canal de comunicación inseguro, sin necesidad de compartir previamente ninguna clave. Para ello, cada parte genera un par de claves pública y privada y comparte por el canal abierto su clave pública; a partir de este intercambio de claves públicas ambas partes calculan de forma independiente un mismo valor secreto.

En la Figura 2-3 se representa el intercambio DH en la versión original de sus autores, que utiliza como grupo cíclico finito el grupo multiplicativo de enteros módulo p , donde p es un número primo grande ($\mathbb{Z}_p$). Los comunicantes deben acordar, en primer lugar, el primo p y un generador g del grupo (todos los elementos del grupo son representables como $g^x \bmod p$). A continuación, cada parte genera sus claves pública y privada para el intercambio; en la figura, $(a, A = g^a \bmod p)$ para el emisor y $(b, B = g^b \bmod p)$ para el receptor. Finalmente, las partes intercambian sus claves públicas A y B , y cada uno calcula el secreto compartido K elevando la clave pública recibida a su propia clave privada: $K = A^b = B^a = g^{ab} \bmod p$.

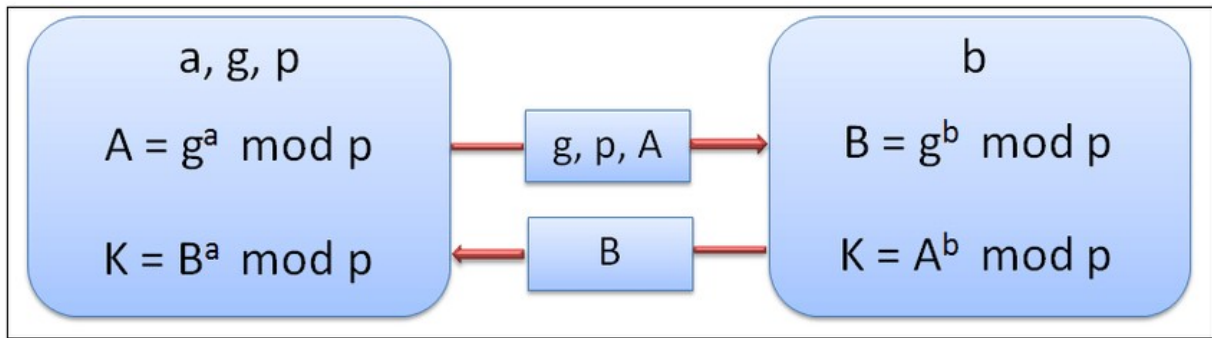


Figura 2-3 Intercambio de clave Diffie Hellman [30]

Aunque los algoritmos PKE y DH garantizan la confidencialidad y resuelven el problema de escalabilidad de los algoritmos simétricos, por sí solos no garantizan la autenticación ni la integridad de los datos [1]. Tal y como se han presentado, los esquemas de cifrado e intercambio de clave son claramente vulnerables frente a ataques de **hombre en el medio**: un adversario capaz de interceptar comunicaciones en el canal y de suplantar la clave pública de uno de los comunicantes legítimos por la suya propia tendría el control total de dichas comunicaciones, pudiendo descifrar, modificar o falsificar los mensajes sin que las partes legítimas se percataran del compromiso. Se analizará más adelante qué medidas se toman para garantizar también autenticación e integridad y evitar este tipo de ataques.

Además, las operaciones de cifrado y descifrado en PKE son significativamente más lentas que las correspondientes de los algoritmos de cifrado simétrico, debido a la mayor complejidad de las operaciones matemáticas involucradas, lo que requiere un mayor tiempo de cómputo. Por ello, los algoritmos de clave pública, como RSA [27] o alternativas como ElGamal [31], rara vez se utilizan para cifrar mensajes directamente en criptosistemas, sino que se combinan con algoritmos de cifrado simétrico en **esquemas híbridos** que aprovechan las ventajas de ambos enfoques. Como se explicará en las secciones 2.5 y 2.6, los algoritmos de clave pública (PKE o DH) se utilizan para intercambiar claves que se utilizan después para proteger el intercambio de datos con criptografía simétrica.

Además de PKE y DH, también es posible utilizar criptografía de clave pública para garantizar la autenticación utilizando **firmas digitales**. Un algoritmo de firma digital es, al igual que los PKE, un algoritmo asimétrico que emplea un par de claves pública y privada, aunque utiliza estas claves de manera diferente. Cualquiera que posea una clave privada puede generar con ella la firma digitalmente de un mensaje, firma cuya validez puede ser verificada por cualquiera con acceso a la correspondiente clave pública. Sin embargo, un adversario que no posea la clave privada no podrá generar firmas válidas para ningún mensaje. En 1991 se estandarizó para firma digital el algoritmo **RSA** en ISO/IEC 9796 [32] y, poco después, en 1994, se estandarizó un esquema de firma basado en ElGamal que se denominó **DSA** (*Digital Signature Algorithm*) en FIPS PUB 186 [33].

Más en detalle, un esquema de firma digital o **DS** (*Digital Signature*) está compuesto por tres funciones: Gen, Sign y Verify. La función $(K_{\text{pri}}, K_{\text{pub}}) = \text{Gen}(s)$ es análoga al caso de PKE descrito anteriormente. La función $\sigma = \text{Sign}(K_{\text{pri}}, m)$ utiliza la clave privada K_{pri} para firmar un mensaje m , generando una firma digital σ asociada al mensaje. Por su parte, la función $\text{Verify}(K_{\text{pub}}, m, \sigma)$ permite verificar si la firma σ corresponde al mensaje m , utilizando la clave pública K_{pub} , o si por el contrario la firma es ilegítima o el mensaje ha sido alterado. Dado que solo el firmante conoce K_{pri} , únicamente él puede generar firmas válidas con la función Sign, mientras que cualquiera que tenga K_{pub} a su disposición puede verificar dichas firmas utilizando la función Verify.

Dado que las funciones Sign y Verify son computacionalmente costosas, especialmente cuando el mensaje a firmar es largo, es práctica habitual que, en lugar de firmar el mensaje completo, **se firme un hash** del mismo [1]. De este modo es posible trabajar con un valor de longitud fija y reducida en lugar de con mensaje completo, lo que optimiza el proceso de firma digital sin comprometer su seguridad. Si denotamos como H a la función *hash*, entonces $\sigma = \text{Sign}(K_{\text{pri}}, H(m))$ es la firma del resumen del mensaje y $\text{Verify}(K_{\text{pub}}, H(m), \sigma)$ comprueba que la firma σ corresponde a dicho resumen, tal y como se ilustra gráficamente en la Figura 2-4.

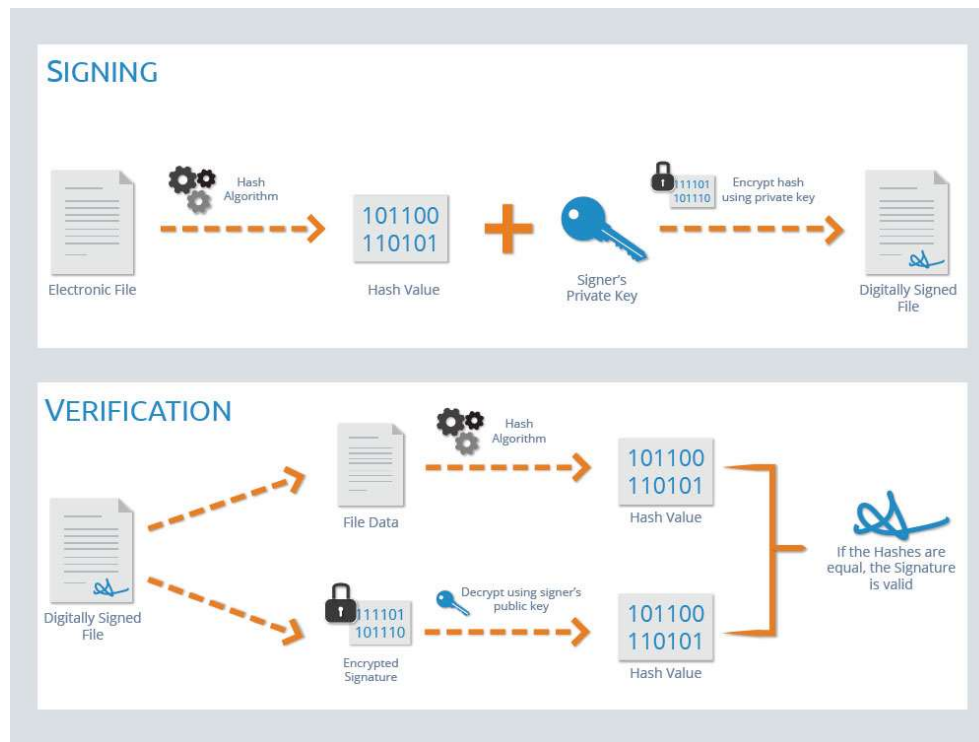


Figura 2-4 Firma digital con algoritmo asimétrico [34]

Con el paso del tiempo, se desarrollaron nuevos algoritmos criptográficos, tanto simétricos como asimétricos. En el ámbito de la criptografía simétrica, el estándar DES fue sustituido por el AES (*Advanced Encryption Standard*) cuando el instituto NIST lo publicó como estándar en FIPS PUB 197 [35]. El algoritmo AES, originalmente llamado Rijndael, admite claves de longitud 128, 192 o 256 bits, lo que le otorga una resistencia significativamente mayor frente a ataques de fuerza bruta que la de DES, cuyo tamaño de clave es de solo 56 bits. Desde entonces, AES se ha consolidado como el algoritmo de cifrado simétrico más utilizado, incluso en la actualidad, aunque no es el único en uso.

Otros algoritmos de cifrado simétrico utilizados actualmente son los finalistas del concurso de evaluación del NIST en el que AES resultó vencedor, TWOFISH, MARS, RC6 y SERPENT [36] [37], así como el algoritmo CAMELLIA, que forma parte del estándar ISO/IEC 18033 [38]; todos ellos con longitudes de clave y niveles de seguridad similares a los de AES. Cabe destacar **CHACHA20** [39], un algoritmo de 256 bits de clave con un diseño más simple que el de AES, lo que le hace muy eficiente y ha impulsado su adopción en los últimos años. Por último, para sistemas embebidos y dispositivos de bajo consumo destaca ASCON [40], un algoritmo de longitud de clave 128 bits muy eficiente que ganó en 2023 el concurso NIST para criptografía ligera [41].

En el ámbito de la criptografía de clave pública, los algoritmos clásicos de cifrado RSA, acuerdo de claves DH y firma digital DSA siguen siendo utilizados en la actualidad. Sin embargo, pero los dos últimos han sido en muchos casos reemplazados por algoritmos basados en curvas elípticas. Los algoritmos de criptografía de curva elíptica (ECC, *Elliptic Curve Cryptography*) [42] ofrecen un nivel de seguridad equivalente a los clásicos, pero con claves de menor longitud y operaciones más eficientes en términos computacionales. Dentro de esta familia destacan el algoritmo acuerdo de claves **ECDH** (*Elliptic Curve Diffie Hellman*) [43] y las firmas digitales **ECDSA** (*Elliptic Curve Digital Signature*) [44] y **EdDSA** (*Edwards-curve Digital Signature Algorithm*) [45]. La seguridad de todos estos algoritmos se basa en la dificultad del problema del logaritmo discreto en grupos finitos.

Los algoritmos de ECC dependen de diferentes **familias de curvas elípticas**, seleccionadas en función de requerimientos normativos y de los requisitos de rendimiento específicos que se pretendan. Destacan dos grandes familias de curvas elípticas: las del NIST, que incluyen **P-256**, **P-384** y **P-521** [43], y las de Edwards, como **Curve25519** y **Curve448** [45]. Las curvas NIST son muy utilizadas por su estandarización y amplio soporte, mientras que las curvas Edwards se imponen en aplicaciones que priorizan la eficiencia computacional. Hay variantes de ECDH tanto con curvas del NIST como con curvas Edwards, mientras que ECDSA emplea solo curvas del NIST y EdDSA utiliza exclusivamente curvas Edwards.

2.3 Seguridad de las primitivas criptográficas

La **seguridad teórica** de los algoritmos criptográficos se refiere a su capacidad para resistir los ataques de un adversario, basándose en los principios matemáticos en los que se fundamentan, sin tener en cuenta factores prácticos como fallos de implementación, errores humanos o una gestión inapropiada de las claves. Existen diferentes definiciones formales sobre seguridad, que se describen en detalle en [1] [3], y con más nivel de formalismo en [2], y distintos modelos para su evaluación. Las definiciones más relevantes se introducen en este apartado.

En el contexto algoritmos de cifrado, la noción más fuerte de seguridad teórica es la **seguridad incondicional** (también conocida como secreto perfecto): la observación del mensaje cifrado no proporciona ninguna información al adversario sobre el mensaje original [1]. Se ha demostrado, desde el punto de vista de la teoría de la información, que esta condición solo puede cumplirse si la longitud de la clave es al igual a la del mensaje y cada clave se utiliza una única vez [46]. Bajo estas condiciones, el algoritmo *One Time Pad* garantiza seguridad incondicional. Sin embargo, otros algoritmos de cifrado simétricos y asimétricos no cumplen con este requisito, pues la observación de cada texto cifrado reduce teóricamente la incertidumbre tanto sobre el mensaje como sobre la clave de cifrado.

Un esquema de cifrado proporciona **seguridad semántica** si cualquier información que un adversario pueda calcular de manera eficiente utilizando el mensaje cifrado también puede calcularse eficientemente sin acceso al mensaje cifrado [3]. Una caracterización formal de la seguridad semántica es la **indistinguibilidad**. Un esquema de cifrado es indistinguible si un adversario no puede distinguir entre dos mensajes cifrados correspondientes a dos mensajes elegidos de manera aleatoria; es decir, dado uno de los cifrados, el adversario no puede adivinar cuál de los dos mensajes originales corresponde al texto cifrado con una probabilidad significativamente mayor que $1/2$. La indistinguibilidad frente a un adversario capaz de realizar los ataques activos CPA, CPA2, CCA y CCA2, definidos en la sección 2.1, se denota como IND-CPA, IND-CPA2, IND-CCA e IND-CCA2, respectivamente.

El concepto equivalente a la indistinguibilidad para algoritmos de firma digital es la **inforjabilidad** (EUF, *Existential UnForgeability*) [2] [47]. Un esquema de firma es inforjable si un adversario no puede calcular la firma digital de un mensaje que no haya sido firmado previamente por la entidad legítima. Este concepto de seguridad se evalúa generalmente en el contexto de un adversario activo capaz de conseguir la firma de mensajes de su elección y de escoger estos mensajes de forma adaptativa, siempre y cuando no sea el mensaje cuya firma quiere falsificar (CMA, *Chosen Message Attack*). La inforjabilidad frente a este adversario se denota como EUF-CMA.

Otra importante noción es la **seguridad computacional**, que evalúa la resistencia de un esquema criptográfico frente a los métodos de ataque más eficientes conocidos teniendo en cuenta los recursos computacionales que un adversario hipotético podría poseer [1]. Un esquema criptográfico se considera computacionalmente seguro si el esfuerzo necesario para comprometer su seguridad excede, por un margen significativo, los recursos computacionales de los que podría disponer un hipotético adversario. A diferencia de la seguridad incondicional, esta noción no garantiza una resistencia absoluta, sino que proporciona un nivel de seguridad adecuado en la complejidad inherente de algunos problemas matemáticos y en el coste computacional que tiene resolverlos.

La seguridad de la gran mayoría de las primitivas, tanto simétricas como asimétricas, se evalúa en términos de seguridad computacional. En el caso de los **algoritmos simétricos**, siempre que no se identifique un ataque criptoanalítico que explote vulnerabilidades en su diseño, su nivel de seguridad viene dado por el esfuerzo requerido para recuperar la clave de cifrado mediante **fuerza bruta**. Por ejemplo, un algoritmo simétrico robusto con una clave de 128 bits ofrece una seguridad computacional equivalente a realizar del orden de 2^{128} operaciones, lejos del alcance de la computación actual.

Por otro lado, en los **algoritmos de clave pública**, la seguridad computacional se basa en la dificultad de resolver problemas matemáticos considerados complejos, como la **factorización** de números grandes en el caso de RSA, el problema del **logaritmo discreto** en el caso de algoritmos como ElGamal y DSA, o el logaritmo discreto en curvas elípticas para ECC. La fortaleza de estos algoritmos depende de que no existan métodos eficientes que permitan resolver los problemas matemáticos subyacentes utilizando los recursos computacionales disponibles para un adversario dentro de un tiempo razonable. En la sección 3.3 se analiza la complejidad de la factorización de claves públicas RSA con el algoritmo GNFS (*General Number Field Sieve*), el más avanzado que se conoce en la actualidad.

Los problemas de factorización y logaritmo discreto son fáciles de formular pero difíciles de resolver cuando los números involucrados son lo suficientemente grandes. La factorización de un entero es el problema bien conocido de encontrar todos sus factores primos. En el cuerpo cíclico finito de los enteros módulo un número primo p , calcular el logaritmo discreto consiste en encontrar el exponente entero x al que hay que elevar un generador g del cuerpo para obtener un valor determinado: dado $N = g^x \bmod p$, encontrar x . Las curvas elípticas también tienen estructura de grupo cíclico finito, y el logaritmo discreto en una curva es el problema de encontrar el factor entero x por el que hay que multiplicar un punto base G de la curva para obtener un punto dado de la misma: dado $N = xG$, encontrar x .

Es importante tener en cuenta que la seguridad computacional basada en problemas matemáticos no implica que exista una demostración formal que establezca que la seguridad de un algoritmo criptográfico se reduce a la dificultad de resolver el problema matemático en el que se fundamenta (lo que se conoce como **seguridad demostrable**). Los algoritmos basados en los problemas de factorización y logaritmo discreto no cuentan con seguridad demostrable, lo que significa que podrían encontrarse ataques más eficientes desde el punto de vista computacional que resolver el problema matemático base.

El nivel de confianza en los algoritmos con seguridad computacional pero no demostrable aumenta con el tiempo y la cantidad de escrutinio por la comunidad científica especializada, por lo que algoritmos como RSA, DSA, DH y sus variantes en ECC, que llevan décadas siendo usados y analizados en busca de vulnerabilidades, se consideran en la actualidad suficientemente seguros. Sin embargo, esta situación podría llegar a cambiar con la disrupción de la **computación cuántica**, un nuevo paradigma de computación que pone en riesgo la seguridad de los algoritmos de clave pública, como se analizará en detalle en la sección 3.

2.4 Arquitectura de protocolos criptográficos

La descripción de **protocolo criptográfico** (o simplemente protocolo) que se presenta en esta sección es la utilizada en las referencias [1] y [3]. Los protocolos se componen de **dos fases** en las que se intercambia información por la red insegura. En la primera fase las partes se autentican y establecen un secreto compartido entre ellas, mientras que en la segunda fase se intercambian datos cifrados y autenticados con claves derivadas de dicho secreto. Se considerarán en este trabajo únicamente protocolos en los que solo intervienen **dos partes** (o comunicantes), a las que se llamará emisor y receptor en función de quién inicia la comunicación.

Se denomina **sesión** a cada instancia que se ejecuta de un protocolo, con sus dos fases, y **clave de sesión** (abreviado como **SK**, de *Session Key*) al secreto compartido de dicha instancia. Es común que en la literatura se abuse del término SK, extendiéndolo también a las claves que se derivan de este secreto para ser usadas por los algoritmos de cifrado y autenticación de los datos que se transmiten durante la sesión, aunque en este trabajo SK solo se referirá al secreto establecido. Por otra parte, se denomina **mensaje** a cada secuencia de datos en claro (es decir, antes de ser cifrados) que se transmite de una vez y **mensaje cifrado** al mensaje ya protegido con claves derivadas de SK.

La Figura 2-5 ilustra esta arquitectura general de un protocolo:



Figura 2-5 Fases de un protocolo criptográfico

Tanto para la autenticación como para el establecimiento de clave de la primera fase, las partes utilizan claves que permanecen válidas durante múltiples sesiones y que se denominan claves permanentes o **claves a largo plazo (LTK, Long Term Key)**. Pueden utilizarse claves permanentes **simétricas**, bien compartidas por las partes o bien con un servidor de claves SK que actúa como tercera parte de confianza, y en este caso se las conoce como PSK (*Pre-Shared Keys*). En ocasiones se utilizan contraseñas en lugar de PSK, que resultan más fáciles de recordar pero que obligan a adaptar los protocolos para evitar que se sean empleadas directamente como claves de los algoritmos por su baja entropía.

Alternativamente, las LTK pueden ser **claves públicas**. En este caso, cada parte posee la componente privada K_{pri} de su clave y comparte la componente pública K_{pub} con la otra, según el esquema clásico de criptografía asimétrica. Lo habitual es que K_{pub} sea públicamente accesible, bien porque se envía directamente en el protocolo o bien porque se incluye en listados de claves de dominio público, por lo que deben estar firmadas por una **tercera parte de confianza**. Es común emplear certificados digitales y autoridades de certificación en infraestructuras de clave pública. Sin embargo, en algunos protocolos las partes pre-comparten sus K_{pub} y no las publican, evitando así la necesidad de firmas digitales y terceras partes en las que confiar.

En la Figura 2-6 se representa gráficamente cómo transcurren las sesiones de un protocolo en el tiempo, cada una asociada a su respectiva clave de sesión. Una propiedad básica que deben cumplir los protocolos es la **frescura de claves** [1], la cual establece que cada clave de sesión SK_i sea única y que un adversario no pueda derivarla a partir de las anteriores $SK_1, SK_2, \dots, SK_{i-1}$. Esta propiedad garantiza que el compromiso de una clave de sesión no afecte a la seguridad de las sesiones siguientes y previene, por ejemplo, frente a ataques de repetición de mensajes cifrados. Para asegurar que las SK son frescas, se utilizan en su algoritmo de derivación, además de las claves de las partes, valores de un solo uso que se intercambian estas durante la fase 1 del protocolo (*nonces*). Estos *nonces* suelen ser valores pseudo-aleatorios, aunque a veces se emplean marcas de tiempo o contadores.

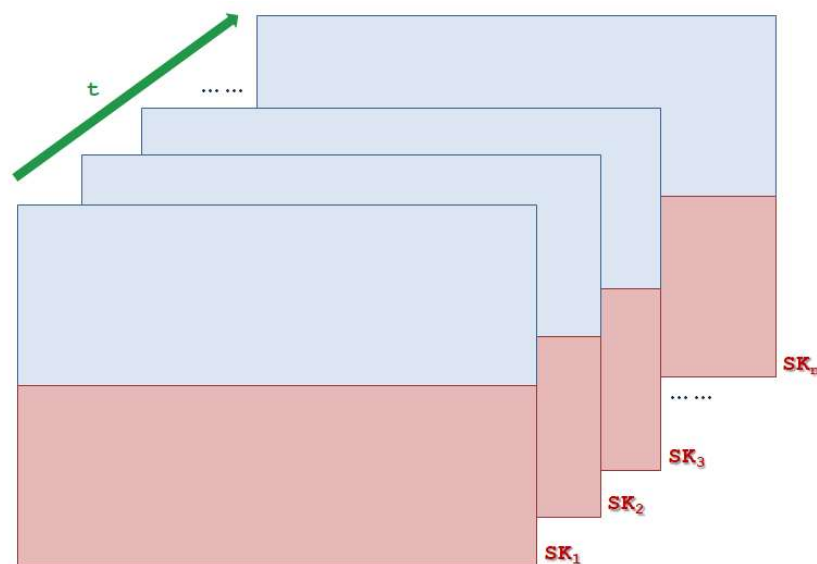


Figura 2-6 Sesiones sucesivas de un protocolo criptográfico

Un requisito más estricto que la frescura para las claves de sesión es el **secreto hacia adelante** [3], también conocido como secreto perfecto hacia adelante o PFS por sus siglas en inglés. Aunque las claves de sesión sean frescas, estas se derivan necesariamente de las claves a largo plazo que comparten los comunicantes, por lo que un compromiso de dichas LTK podría llegar a revelar todas las SK. Un protocolo proporciona secreto hacia adelante cuando esto no ocurre, es decir, si el compromiso de las claves a largo plazo no revela las claves de sesión establecidas previamente a partir de ellas.

La componente utilizada por los protocolos para garantizar el secreto hacia adelante son las **claves públicas efímeras (EK, *Ephemeral Keys*)**. Estas claves se generan dinámicamente en cada ejecución del acuerdo de claves y se utilizan exclusivamente para la correspondiente sesión, combinadas de algún modo con las LTK para la derivación de la SK. Inmediatamente después se eliminan de manera segura (en las implementaciones robustas, la componente privada de la clave privada nunca se almacena de forma persistente y solo permanece en memoria el tiempo estrictamente necesario para completar la derivación de la clave de sesión). Aunque las LTK fueran comprometidas, las SK establecidas previamente permanecerían seguras porque las correspondientes EK no podrían recuperarse.

A continuación, se analizan en detalle cada una de las dos fases de un protocolo criptográfico.

2.5 Autenticación y establecimiento de clave (fase 1)

Se denomina **establecimiento de clave** a cualquier proceso mediante el cual una clave secreta compartida se pone a disposición de dos o más partes para su posterior uso criptográfico [1]. Este proceso resulta fundamental para garantizar la seguridad de las comunicaciones en Internet, una red abierta en la que los comunicantes típicamente no tienen una relación de confianza entre sí. En lo que sigue, se centrará la atención en el establecimiento de claves entre **dos partes**, dado que es el escenario más simple y a la vez el de uso más extendido.

Es habitual diferenciar dos tipos de establecimiento de claves (entre dos partes): transporte y acuerdo. En el **transporte de claves** una de las partes genera u obtiene un valor secreto y lo envía de manera segura a la otra parte, mientras que en el **acuerdo de claves** ambas partes derivan un secreto compartido a partir de información asociada con cada una de ellas (de tal manera que ninguna pueda calcular el secreto de antemano). En ambos casos, en cada instancia del proceso de establecimiento se establece una nueva clave de sesión, que habitualmente es fresca en el sentido que se explicó en el apartado anterior [1].

El objetivo de la fase 1 de los protocolos criptográficos no es solo establecer la clave de sesión, sino que también se pretende que los comunicantes se autentifiquen, evitando así que un adversario pueda suplantar a una de las partes legítimas, y es por ello que se la suele denominar **AKE (*Authenticated Key Establishment*)** en la literatura. La autenticación en el protocolo puede ser mutua o unidireccional, siendo este último caso el que ocurre por ejemplo en algunos protocolos de tipo cliente-servidor en los cuales solo el servidor se autentica ante el cliente.

Existe una gran variedad de protocolos de este tipo. El AKE puede construirse utilizando **primitivas simétricas o asimétricas**, siendo este último caso el más común. Además, puede implicar o no la participación de una **tercera parte de confianza (TTP, *Trusted Third Party*)**, que puede estar fuera de línea o en línea. En [3] los autores realizan un repaso exhaustivo de los diferentes tipos de protocolo criptográfico que se pueden construir combinando estas alternativas; a continuación, se describen los más relevantes en el contexto de comunicaciones seguras en Internet.

En los **AKE basados en criptografía simétrica que no dependen de TTP**, las partes deben haber pre-compartido una clave simétrica por un canal seguro. En estos protocolos, la autenticación de las partes suele ser mutua y se basa principalmente en demostrar que ambas partes están en posesión de la PSK. Existen multitud de protocolos de este tipo, tanto para el transporte como para el establecimiento de claves de sesión; muchos de ellos garantizan la frescura de las claves, pero ninguno ofrece secreto hacia adelante, ya que no involucran claves efímeras. A pesar de esta limitación, muchos protocolos notables de Internet, como IPSEC, TLS y SSH, incluyen la opción de usar PSK como AKE por su simplicidad, así como protocolos en los que el acceso se basa en una contraseña de usuario, como por ejemplo WPA2, WPA3 y Bluetooth.

También se utilizan **AKE basados en criptografía simétrica con TTP**, tercera parte que en este caso debe estar en línea. El TTP es un servidor que autentica a las partes involucradas en la comunicación y distribuye claves de sesión en tiempo real a los participantes de la red. Para ello, el servidor mantiene una base de datos de PSK asociadas a cada participante en la red. Este tipo de protocolos tampoco tiene la propiedad de secreto hacia adelante. Los ejemplos más conocidos son Kerberos [48], un protocolo de transporte de clave habitual en redes corporativas, y EAP-SIM [49] o EAP-AKA' [50], protocolos de acuerdo de clave empleados en redes de telefonía móvil 3G, 4G y 5G (en estos dos últimos la PSK corresponde a la clave almacenada en la tarjeta SIM o USIM del dispositivo móvil).

En Internet, los protocolos basados en clave pública son mucho más populares que los protocolos basados en criptografía simétrica, ya que la clave pública evita la necesidad de que las partes compartan un secreto antes de iniciar la comunicación o de disponer de un TTP en línea disponible durante la misma. Además, la clave pública permite dotar a los protocolos de propiedades de seguridad avanzadas, como el secreto hacia adelante. Los AKE basados en criptografía asimétrica pueden depender o no de una tercera parte de confianza, que en este caso suele estar fuera de línea: la TTP no participa directamente en el AKE, sino que actúa de forma previa para garantizar la validez de las claves públicas que utilizan las partes.

Esta garantía de validez de las claves públicas se realiza habitualmente mediante una infraestructura de clave pública (**PKI**, por sus siglas en inglés), que proporciona un marco estandarizado para la gestión de claves públicas y certificados digitales [51]. En esta infraestructura, una Autoridad de Certificación (CA, *Certification Authority*) emite certificados digitales que vinculan cada clave pública con la identidad de su propietario (nombre, dirección de correo electrónico, dominio de Internet, etc.), después de verificar que el propietario de la clave es quien afirma ser. La CA firma digitalmente el certificado con su clave privada y hace accesible su clave pública para que cualquiera pueda verificar la firma y comprobar que el certificado no ha sido alterado y que proviene de una CA confiable.

Un matiz importante respecto de las PKI es que no siempre funcionan completamente fuera de línea. Aunque este es el caso para la emisión de certificados y, en este sentido, no es necesaria la participación de la CA en los protocolos criptográficos, los certificados emitidos pueden ser revocados y las partes deben tener mecanismos que les permitan verificar si un certificado sigue siendo válido. Para ello, es posible descargar las listas de revocación (CRL, *Certificate Revocation List*) o utilizar el protocolo OCSP (*Online Certificate Status Protocol*) para consultar dinámicamente con la CA si un certificado específico ha sido revocado o sigue siendo confiable [51] [52].

Aunque la PKI es la opción de TTP más frecuente en Internet, existen modelos más sencillos que pueden emplearse en redes de comunicación pequeñas o cuando los participantes tienen algún tipo de relación y pueden confiar en una verificación de claves entre ellos. Un ejemplo de ello es la llamada red de confianza (**WoT**, *Web of Trust*), popularizada por la aplicación PGP/GPG y el protocolo de correo electrónico cifrado S/MIME [21] [23] [53]. En WoT no existe un TTP centralizado en el que confíen los participantes de la red y, en su lugar, unos usuarios firman las claves públicas de otros, validando su autenticidad en función de su confianza mutua. Cada usuario decide en qué claves confiar basándose en el número y la reputación de las firmas que ha recibido de otros usuarios.

Cabe mencionar también que, en algunos protocolos, las partes comparten directamente sus claves públicas, ya sea en bruto o como certificados autofirmados (**PSK**). Siempre que el intercambio inicial de claves públicas se realice a través de un canal seguro, este mecanismo proporciona una forma ágil y sencilla de establecer un AKE, ya que elimina la necesidad de la intervención de una tercera parte de confianza. Por ejemplo, funcionan de este modo la red privada virtual WIREGUARD [12], que emplea como AKE una instancia del protocolo Noise [54] con PSK, al igual que la aplicación de acceso remoto SSH [20], cuyo AKE también se basa en el intercambio directo de claves públicas.

Independientemente del método que se utilice para garantizar la validez de las claves públicas, el establecimiento de clave basado en criptografía de clave pública puede ser tanto por transporte como por acuerdo. Sin embargo, **el método de transporte ha caído en desuso** en protocolos de Internet basados en clave pública, siendo su presencia cada vez menor. Por ejemplo, las versiones de los protocolos IPSEC, TLS y SSH de hace algunos años aún contemplaban mecanismos de transporte basados en cifrado RSA, pero en las versiones más recientes de estos protocolos esta funcionalidad ha desaparecido (IPSEC y TLS) o bien está marcada como obsoleta (SSH).

La razón principal de esta tendencia es que **el acuerdo de claves ofrece mayores garantías de seguridad**. Por un lado, el transporte de claves no proporciona secreto hacia adelante dado que no se emplean claves efímeras en uso, al contrario que en un acuerdo de claves, que puede combinar claves públicas LTK y EK para garantizar esta propiedad. Por otro, el transporte resulta completamente vulnerable al compromiso de la clave privada del receptor, ya que su conocimiento permite descifrar todas las KS que hayan sido transmitidas cifradas con la clave pública correspondiente (e incluso las KS que se transmitan en el futuro, si el compromiso pasa inadvertido a las partes).

Para el acuerdo de claves se utilizan **primitivas criptográficas basadas en DH y ECDH**, siendo esta última más empleada debido a su mayor eficiencia computacional y menor consumo de recursos. Así ocurre, por ejemplo, en los protocolos IPSEC, OPENVPN, WIREGUARD, TLS, DTLS, QUIC, SSH y SIGNAL, empleados en distintas capas del modelo TCP/IP, en los que las claves de sesión se derivan utilizando este tipo de primitivas.

Para garantizar el **secreto hacia adelante**, los esquemas AKE basados en clave pública combinan claves efímeras con claves de largo plazo para derivar la clave de sesión. Durante cada instancia de AKE, las partes intercambian las claves públicas de las EK generadas y, para conseguir autenticación, las claves públicas LTK o información derivada de ellas. Cada parte calcula la SK combinando su clave privada efímera con la clave pública efímera de la otra parte mediante primitivas criptográficas basadas en DH o ECDH, y añade información derivada de las LTK para vincular la SK con las identidades de las partes involucradas.

2.6 Intercambio de datos cifrados y autenticados (fase 2)

Una vez que las partes han compartido una clave de sesión comienza el intercambio de datos por el canal inseguro. Los mensajes que se transmiten por este canal se cifran para garantizar su **confidencialidad** y, además, se les adjunta un *tag* que asegura que su origen es el esperado (es decir, **autentica el origen de datos**). El legítimo receptor de un *tag* puede volver a calcularlo a partir del mensaje y comprobar si coincide con el valor recibido. Este mecanismo de autenticación no solo asegura el origen de los datos sino también su **integridad**, ya que si un adversario modifica un mensaje provocará un fallo en la verificación de la autenticación a partir del *tag*.

Ambos procesos criptográficos, cifrado y autenticación, utilizan **claves derivadas** de la clave de sesión, que normalmente son diferentes. Además, es práctica común emplear claves de cifrado diferentes para cada sentido de la comunicación con el fin de limitar el acceso de un adversario que logre comprometer la clave de uno de los sentidos, así como para evitar los ataques de repetición. La derivación de claves suele combinar la clave de sesión con los *nonces* del AKE y diferentes etiquetas en función de la clave que se deriva (típicamente se usan construcciones basadas en HMAC, que se verá a continuación).

Respecto al cifrado de los datos, como las partes disponen de una clave compartida es habitual utilizar algoritmos de **cifrado simétrico**, mucho más eficientes que los PKE. Por otro lado, la construcción habitual para calcular el *tag* de un mensaje es el **MAC** (*Message Authentication Code*), que puede entenderse como una generalización de las funciones *hash* haciendo intervenir una clave [1] [55]. Más formalmente, un código MAC es una familia de funciones parametrizadas por una clave k tal que $\text{MAC}_k(m)$ toma un mensaje m de longitud arbitraria y genera un *tag* de longitud fija. Dados k , $\{m_1 m_2 \dots m_L\}$ y $\{\text{MAC}_k(m_1) \text{MAC}_k(m_2) \dots \text{MAC}_k(m_L)\}$, es computacionalmente difícil encontrar $\text{MAC}_k(m)$ para $m \notin \{m_1 m_2 \dots m_L\}$ cualquiera que sea el valor de L .

Es posible construir códigos MAC a partir de cifradores en bloque o de funciones *hash*, aunque las versiones modernas de los protocolos criptográficos han apostado por la segunda opción. Es común encontrarse con la construcción **HMAC** (*Hash MAC*) [55], usada con las funciones *hash* SHA-1 o SHA-2, aunque se trata de un esquema genérico válido para cualquier *hash*. Existe otra construcción específica para las funciones SHA-3, denominada **KMAC** (*Keccak MAC*) [56], así como una construcción basada en cifradores en bloque llamada **CMAC** (*Cipher-based MAC*) [57]. Sin embargo, estas alternativas no han llegado a implementarse hasta ahora en protocolos criptográficos debido a que el HMAC está muy consolidado, es eficiente y se considera suficientemente seguro.

Independientemente del tipo de MAC utilizado, es posible combinarlo con la función de cifrado de diferentes modos, y no todos ellos exhiben las mismas propiedades de seguridad. La combinación de las funciones de cifrado y autenticación se suele denominar como **cifrado autenticado** (AE, *Authenticated Encryption*). La combinación **encrypt-then-MAC**, en la que primero se cifra el mensaje y después se calcula el MAC del cifrado, resulta ser la más segura porque cualquier manipulación del cifrado puede ser detectada por los legítimos comunicantes [2] [58]. Este modo es usado, por ejemplo, en IPSEC.

Los modos **MAC-then-encrypt** usado en TLS-1.2 (se calcula primero el MAC del mensaje y se cifra la concatenación de mensaje y *tag*) y **encrypt-and-MAC** usado en SSH (el MAC del mensaje se adjunta directamente a su cifrado), sin embargo, no garantizan algunas propiedades deseables como la confidencialidad bajo ataque de texto cifrado elegido. Además, en el modo **encrypt-and-MAC** el *tag* puede llegar a revelar información del mensaje si no se añade algún vector inicial o contador en su cálculo [58]. Aunque **MAC-then-encrypt** y **encrypt-and-MAC** no pueden considerarse formalmente seguros en general, sí lo son bajo ciertas suposiciones respecto a cómo se codifican los datos y las funciones de cifrado y MAC empleadas [59] [60].

Alternativamente, es posible construir esquemas de cifrado autenticado que no requieren la combinación de dos funciones separadas, cifrado y MAC. Estos esquemas generan tanto el texto cifrado como el *tag* de autenticación de una sola vez y utilizando una única clave, lo cual ofrece mejoras significativas en términos de eficiencia y aporta mayor simplicidad al proceso criptográfico. El cifrado autenticado más utilizado de este tipo es **AES-GCM** (*Galois Counter Mode*) [61], una variante del cifrado AES-CTR a la que se añade una función hash universal definida sobre un campo de Galois binario para la autenticación de datos.

El algoritmo AES-GCM resulta mucho más eficiente que los modos combinados de AES con HMAC, principalmente porque cifrado y autenticación se realizan en un único proceso, reduciendo así el número de operaciones necesarias. Además, el modo contador es completamente paralelizable y el cálculo del *tag* es muy eficiente, mientras que HMAC procesa los bloques de manera secuencial y no es paralelizable. Por otra parte, algunas arquitecturas incluyen optimizaciones específicas para AES-GCM, como las extensiones AES-NI (cifrado y descifrado AES) y la instrucción PCLMULQDQ (multiplicación sin acarreo en campos de Galois) de los procesadores Intel y AMD modernos [62].

Existen muchos otros modos de encadenamiento capaces de realizar cifrado autenticado, como por ejemplo IAPM, XECB, OCB, EAX, CWC y CCM [63], aunque el único de estos que se utiliza como alternativa a AES-GCM en algunos protocolos criptográficos como IPSEC y TLS-1.3 es **AES-CCM** (*Counter with CBC-MAC*) [64]. AES-CCM también se basa en AES-CTR para el cifrado, pero implementa un MAC basado en el modo de encadenamiento CBC para calcular el *tag* de autenticación. Aunque CBC-MAC es más sencillo de implementar que GCM, resulta menos eficiente en procesadores con AES-NI y PCLMULQDQ.

A pesar de que los modos de encadenamiento GCM y CCM son válidos para cualquier cifrador en bloque de 128 bits, en la práctica solo se utilizan con AES. Con el objeto de contar con una alternativa eficiente a AES-GCM y AES-CCM, lo que podría ser necesario si llegara a encontrarse un criptoanálisis de AES, se diseñó **CHACHA20-POLY1305** [39]. Este algoritmo cifra con el algoritmo de flujo CHACHA20, que ejecuta 20 rondas de permutación, y simultáneamente calcula el *tag* de autenticación con el algoritmo POLY1305, basado en aritmética modular con el número primo $2^{130}-5$. CHACHA20-POLY1305 es mucho más eficiente que AES-GCM cuando no se emplea aceleración hardware, pero menos en este caso.

Finalmente, los paquetes que se intercambian en los protocolos criptográficos no solo incluyen el mensaje cifrado y el *tag*, sino también algunos campos adicionales como el contador de paquete, el identificador de la sesión o valores de *nonce* o IV para el cifrado autenticado, que conforman lo que se denomina cabecera del paquete. Aunque esta cabecera no se cifra, se debe garantizar su autenticación. Los esquemas de cifrado autenticado que permiten este comportamiento se conocen como **AEAD** (*Authenticated Encryption with Associated Data*).

Los algoritmos AES-GCM, AES-CCM y CHACHA20-POLY1305 son de este tipo, así como algoritmos implementados en algunos protocolos a partir de los modos combinados *encrypt-then-MAC*, *MAC-then-encrypt* y *encrypt-and-MAC* para contar también con esta funcionalidad. La Tabla 2-1 muestra ejemplos de protocolos criptográficos que soportan estos esquemas de cifrado autenticado.

Esquema	Protocolos
AES-GCM	WPA2, WPA3, BLUETOOTH, ZIGBEE, IPSEC, OPENVPN, WIREGUARD, TLSv1.2, TLSv1.3, QUIC, SSH, SIGNAL
AES-CCM	WPA2, WPA3, BLUETOOTH, ZIGBEE, IPSEC, TLSv1.2
CHACHA20-POLY1305	OPENVPN, WIREGUARD, TLSv1.3, QUIC, SSH, SIGNAL
encrypt-then-HMAC	IPSEC
encrypt-and-HMAC	SSH
HMAC-then-encrypt	TLSv1.2

Tabla 2-1. Esquemas de cifrado autenticado soportados por protocolos criptográficos

3 AMENAZA Y RESISTENCIA CUÁNTICAS

En esta sección se presenta la amenaza que supone el desarrollo de la computación cuántica para los criptosistemas actuales, principalmente para los algoritmos de clave pública, cuyo uso hoy día resulta fundamental para garantizar la seguridad de Internet. Se explican los principios básicos de la computación cuántica y se presentan los algoritmos cuánticos de Shor y Grover, que son los más relevantes desde un punto de vista criptográfico.

Seguidamente, se revisa el progreso de la computación cuántica y se hace una prospectiva sobre el camino que queda por recorrer para la construcción de un ordenador cuántico universal capaz de vulnerar la seguridad de los criptosistemas actuales. A pesar de los avances en el desarrollo de esta tecnología, aún quedan problemas importantes por resolver, por lo que resulta improbable que esto ocurra en la próxima década, opinión mayoritariamente aceptada en la comunidad científica especializada.

Finalmente, se describen las dos líneas de trabajo que se están siguiendo para resistir a la amenaza cuántica: la criptografía cuántica, sobre todo el intercambio cuántico de claves, y la criptografía post-cuántica. Se destaca la importancia de avanzar en la transición hacia estos nuevos esquemas criptográficos, a pesar de que la materialización de la amenaza no parece cercana, tanto por el elevado riesgo que se asume al seguir utilizando criptosistemas potencialmente vulnerables como porque dicha transición será compleja y llevará tiempo.

3.1 La amenaza cuántica a los criptosistemas

El instituto estadounidense NIST describió de forma completa y concisa en qué consiste la **amenaza cuántica** a los criptosistemas cuando en diciembre del 2016 publicó su concurso para definir algoritmos criptográficos post-cuánticos [65]. El inicio de dicha convocatoria afirma:

“En los últimos años, ha habido una cantidad sustancial de investigación sobre computadoras cuánticas, máquinas que explotan fenómenos de mecánica cuántica para resolver problemas matemáticos que son difíciles o intratables para las computadoras convencionales. Si alguna vez se construyen computadoras cuánticas a gran escala, comprometerán la seguridad de muchos algoritmos criptográficos de uso común.

En particular, las computadoras cuánticas romperían por completo muchos criptosistemas de clave pública, incluidos RSA, DSA y criptosistemas de curva elíptica. Estos criptosistemas se utilizan para implementar firmas digitales y establecimiento de claves y desempeñan un papel crucial para garantizar la confidencialidad y autenticidad de las comunicaciones en Internet y otras redes. [...]”

Han pasado 8 años desde entonces y la amenaza que describía NIST sigue estando vigente, si cabe con mayor peso dado que en este periodo se han producido avances notables en el **desarrollo de la computación cuántica** y las grandes potencias mundiales, sobre todo Estados Unidos y la República Popular China, continúan invirtiendo ingentes cantidades de dinero en la investigación y el desarrollo de ordenadores cuánticos.

La eventual construcción de un ordenador cuántico suficientemente potente y preciso pondría en jaque la seguridad de los criptosistemas de clave pública en uso actualmente para garantizar la seguridad de las comunicaciones en Internet. Cualquier actor que llegara a contar con dicha capacidad podría **vulnerar los mecanismos de cifrado** que protegen la confidencialidad de la información que se transmite en Internet. Además, tendría la capacidad de falsificar mensajes e incluso suplantar a las partes comunicantes vulnerando los mecanismos de integridad y autenticación en uso.

El alcance de esta amenaza es considerable, ya que la confianza que la sociedad actual ha depositado en la tecnología digital es un pilar fundamental de nuestro estilo de vida, y hemos llegado a un escenario en el que todo, personas y dispositivos, está conectado. Valga como ejemplo la explosión del Internet de las cosas en la última década. Utilizamos a diario Internet de forma consciente para comprar, acceder al banco, comunicarnos, establecer redes sociales, etc., y quizá menos conscientemente para poder disfrutar de servicios esenciales como el suministro energético o las redes de transporte.

Cada vez hay mayor conciencia de la necesidad de **protegerse cuanto antes** ante la posibilidad de que la computación cuántica avance lo suficiente como para vulnerar los criptosistemas actuales [66]. El riesgo no afecta únicamente a la información que pudiéramos llegar a compartir en un futuro escenario cuántico, sino también a la que intercambiamos hoy en día. En efecto, existe la posibilidad de que un actor malicioso esté interceptando y almacenando las comunicaciones actuales con el fin de descifrarlas cuando pueda tener acceso a un ordenador cuántico capaz, aproximación conocida como ‘cosecha-ahora-descifra-después’.

Se explicará en los siguientes apartados por qué los ordenadores cuánticos son potencialmente capaces de vulnerar los criptosistemas de clave pública actuales (implementando ciertos algoritmos cuánticos), cuán lejano está el desarrollo de ordenadores cuánticos capaces de ello y qué medidas se están adoptando para resistir y evitar el riesgo cuántico al que nos enfrentamos (comunicaciones cuánticas y criptografía post-cuántica).

3.2 Computación multidimensional y algoritmos cuánticos

La **computación cuántica** se basa en aprovechar las propiedades de la mecánica cuántica para realizar cálculos de manera más eficiente que los ordenadores tradicionales. Para ello utiliza tanto dispositivos especializados como algoritmos específicos que aprovechan los fenómenos cuánticos, fundamentalmente la superposición de estados y el entrelazamiento cuántico, para resolver problemas complejos que los ordenadores clásicos no pueden abordar en un tiempo razonable [67]. En la Figura 3-1 se puede ver un ordenador cuántico desarrollado por la multinacional IBM.

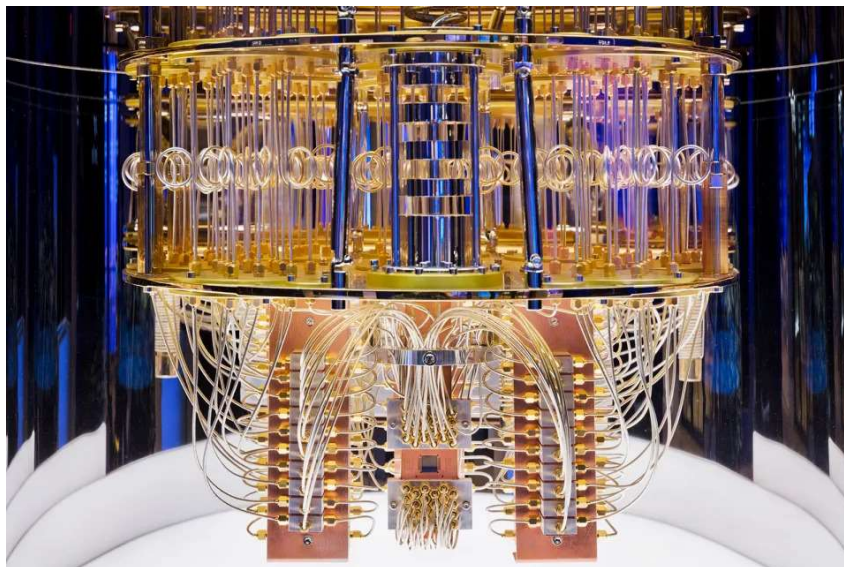


Figura 3-1 Ordenador cuántico de IBM en 2021 [69]

Mientras que un ordenador clásico utiliza bits como unidades básicas de información, el ordenador cuántico emplea **qubits** (abreviatura de quantum bits). Un bit clásico puede representar únicamente dos estados, 0 o 1, y típicamente se implementa a través de un impulso eléctrico u óptico en los sistemas de telecomunicaciones e informática actuales. Por otra parte, los qubits son sistemas cuánticos que se implementan mediante sistemas físicos naturales (iones atrapados, átomos de Rydberg o fotones) o artificiales (uniones Josephson o puntos cuánticos) y que se pueden controlar de manera individual. Como ocurre con los bits, cada qubit puede adoptar también solo dos estados fundamentales, $|0\rangle$ y $|1\rangle$, pero los qubits exhiben además las propiedades fundamentales de la mecánica cuántica como la superposición y el entrelazamiento [67] [68].

El fenómeno de la **superposición** (también conocido como dualidad onda-corpúsculo) permite a un qubit estar en múltiples estados simultáneamente. Las partículas se comportan como las ondas clásicas, que pueden descomponerse en una suma o superposición de varias ondas puras de frecuencia definida mediante la transformada de Fourier. Por otra parte, el **entrelazamiento** es un tipo de patrón de interferencia cuántico, sin análogo clásico, que correlaciona los estados de dos o más partículas de manera que la medición de un estado afecta a los demás estados ligados a él. El entrelazamiento permite que los estados de los qubits de un sistema cuántico sean dependientes entre sí, incluso si se encuentran muy separados entre sí.

Un conjunto de qubits en superposición permite crear un **espacio computacional multidimensional**, trascendiendo la computación binaria basada en bits que implementan los ordenadores clásicos. Mientras que utilizando n bits solo se puede representar uno de los 2^n estados posibles a la vez, un conjunto de n qubits en superposición puede representar los 2^n estados a la vez. Esto se debe a que, en lugar de estar en un estado definido de 0 o 1 como un bit, cada qubit en superposición puede encontrarse en un estado de 0, en un estado de 1, o en una superposición de ambos (su estado se representa mediante una función de onda que captura las probabilidades asociadas a los estados base 0 y 1). Idealmente cada uno de los qubits permanece en este estado superpuesto y solo colapsa al valor concreto 0 o 1 en el momento en que se mide [68].

La siguiente imagen representa esta idea gráficamente.

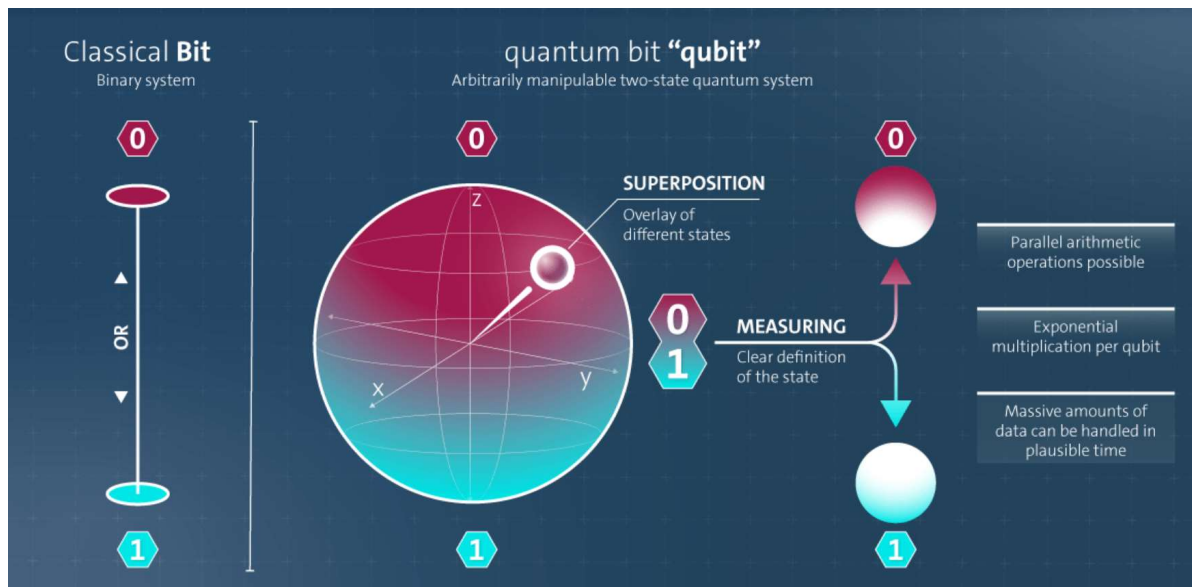


Figura 3-2 Representación gráfica de un qubit y sus propiedades [70]

La capacidad de los ordenadores cuánticos para trabajar con múltiples estados simultáneamente les permite procesar una enorme cantidad de información en paralelo. En la medición tras el procesado es cuando se recupera únicamente uno de los estados de la superposición. Esto otorga a la computación cuántica el potencial de superar exponencialmente a la computación clásica en la resolución de determinados problemas complejos, algunos de los cuales se consideran intratables con los ordenadores clásicos. Para aprovechar estas ventajas son necesarios algoritmos específicos que puedan ejecutarse en este tipo de ordenadores y aprovechar el modelo de computación multidimensional que ofrecen los qubits (es decir, **algoritmos cuánticos**).

Los primeros pasos en el desarrollo de la computación cuántica tuvieron lugar en el ámbito de la física teórica a comienzos de la década de 1980. Richard Feynman argumentó que la simulación de sistemas cuánticos podría beneficiarse de un ordenador basado en fenómenos cuánticos [71], Paul Benioff introdujo el concepto de máquina de Turing cuántica [72] y David Deutsch definió el ordenador cuántico universal [73]. Sin embargo, hubo que esperar hasta la década de 1990 para que se desarrollaran los primeros algoritmos cuánticos a partir de estos fundamentos teóricos.

El investigador Michele Mosca recopila en un extenso artículo los algoritmos cuánticos clásicos [74]. Los más relevantes son el de **Deutsch-Jozsa** (1992), que determina si una función es constante o balanceada; el de **Simon** (1994), diseñado para identificar un patrón oculto en una función binaria; el de **Shor** (1994), para factorización de números enteros, el de **Grover** (1996), de búsqueda en una lista no ordenada; el de **Bernstein-Vazirani** (1997), una generalización del de Deutsch-Jozsa para encontrar un patrón oculto en una función lineal; el de **Nielsen-Chuang** (1996), que desarrolla la versión cuántica de la transformada de Fourier y se usa por muchos otros algoritmos (por ejemplo, Shor y simulaciones cuánticas) para extraer información precisa sobre el estado del sistema cuántico.

El primer algoritmo cuántico que se implementó experimentalmente fue el Deutsch-Jozsa en 1998. Un grupo de investigación que lideraban Neil Gershenfeld e Isaac Chuang del MIT implementó el algoritmo utilizando un sistema de resonancia magnética nuclear para manipular el estado cuántico de moléculas de cloroformo [75]. Este hito demostró experimentalmente que las bases de la computación cuántica eran correctas.

Poco después, en el año 2001, un grupo de investigación de la empresa IBM logró **implementar el algoritmo de Shor** en un sistema cuántico también basado en resonancia magnética nuclear con 7 qubits, consiguiendo factorizar el número 15 en sus factores primos 3 y 5 [76]. Aunque el alcance de este experimento fue limitado, se considera otro hito fundamental en el desarrollo de la computación cuántica, ya que por primera vez logró implementarse un algoritmo capaz de resolver un problema exponencialmente más rápido que en un ordenador clásico.

Desde entonces se han desarrollado notablemente los sistemas cuánticos y, como consecuencia, la investigación en computación cuántica ha tenido un avance considerable, tanto en la definición de nuevos algoritmos como en su implementación. La comunidad científica ha intensificado su interés en las posibilidades que ofrece la computación cuántica, desarrollando nuevos algoritmos para llegar más lejos en campos como la simulación de sistemas físicos [77], el aprendizaje automático [78] o el criptoanálisis de algoritmos post-cuánticos [79]. Se incidirá sobre este último punto en las siguientes secciones.

En lo que se refiere a la seguridad de los criptosistemas actuales, los algoritmos cuánticos que tienen un impacto directo son los de Shor y Grover, principalmente el primero. En las siguientes secciones se describen estos algoritmos y se analiza su impacto en la seguridad de los algoritmos de clave pública, en los algoritmos de cifrado simétrico y en las funciones hash.

3.3 El algoritmo de factorización de Shor

En 1994 Peter Shor publicó su famoso artículo “*Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*” [80], en el que se describe un algoritmo cuántico capaz de resolver los problemas de la **factorización entera** y de cálculo de **logaritmos discretos** en tiempo polinomial en un hipotético ordenador cuántico.

Estos dos problemas matemáticos son la base de la seguridad de los algoritmos criptográficos de clave pública en uso a día de hoy, ya que se consideran intratables con las capacidades de computación clásicas para instancias de tamaño suficientemente grande. Tal es el caso del algoritmo RSA, cuya seguridad se basa en la dificultad de factorizar un producto de dos números primos grandes [28]. También para el esquema de acuerdo de claves DH y el algoritmo de firma digital DSA, así como para sus equivalentes en curva elíptica ECDH y ECDSA, ya que para todos ellos la seguridad radica en la dificultad de calcular logaritmos discretos en grupos finitos [33] [42].

El algoritmo clásico más eficiente que se conoce para resolver estos problemas cuando el número es grande es la criba general en campos numéricos, conocido como **GNFS** por sus siglas en inglés [81]). Para el problema de factorización de un entero N , la complejidad de GNFS viene dada por la expresión $\exp[(64/9)^{1/3} (\ln N)^{1/3} (\ln \ln N)^{2/3}]$, por lo que su tiempo de ejecución crece de manera sub-exponencial con $\log_2(N)=\ln(N)/\ln(2)$, el número de bits necesarios para representar N [82].

Cabe destacar que, aunque desde su la definición de GNFS se han introducido numerosas mejoras y optimizaciones en sus implementaciones, solo han logrado reducir ligeramente la constante 64/9 y no cambiar la naturaleza subexponencial del algoritmo. El mayor módulo RSA cuya factorización con GNFS se ha reportado hasta la fecha es RSA-250, un entero con 250 dígitos decimales o 829 bits [83]. Este hito, que se alcanzó en 2020, aún dista mucho de los valores usados en los algoritmos de clave pública actualmente.

La relevancia del algoritmo cuántico de **Shor** radica en su capacidad para resolver en un tiempo razonable los problemas de factorización entera y logaritmo discreto, que son intratables para algoritmos como GNFS en ordenadores clásicos. De hecho, la **complejidad** del algoritmo de Shor para factorizar un número entero N viene dada por la expresión $O[(\log_2 N)^3]$, por lo que su tiempo de ejecución crece de manera **polinómica** con el número de bits de N [74] [80]. En la Tabla 3-1 se puede ver la diferencia significativa entre las complejidades de GNFS y de Shor cuando crece el tamaño de N .

Bits N	Complejidad GNFS	Complejidad Shor
256	$1,63 \times 10^{21}$	$1,68 \times 10^7$
512	$8,09 \times 10^{28}$	$1,34 \times 10^8$
1024	$1,18 \times 10^{39}$	$1,07 \times 10^9$
2048	$2,86 \times 10^{52}$	$8,59 \times 10^9$
3072	$1,44 \times 10^{62}$	$2,90 \times 10^{10}$
4096	$1,09 \times 10^{70}$	$6,87 \times 10^{10}$

Tabla 3-1. Crecimiento de las complejidades de GNFS y Shor

Para lograr esta mejora significativa, el algoritmo de Shor aprovecha la capacidad de computación multidimensional que ofrecen los qubits. Este algoritmo reduce el problema de encontrar factores de un número N al de calcular el **orden** de un elemento módulo N impar, un problema cuya resolución con recursos computacionales clásicos resulta ser muy ineficiente pero que se ajusta muy bien al modelo de computación cuántica.

Veamos en qué consiste este cambio de enfoque. En primer lugar, se selecciona un entero $1 < \alpha < N$ que sea coprimo con N , para lo cual se comprueba clásicamente que su máximo común divisor (mcd) es 1 (para N suficientemente grande, la probabilidad de que un α escogido aleatoriamente sea coprimo con N es alta). A continuación, se ejecuta la componente cuántica del algoritmo, el cálculo del orden de α , esto es, el menor r tal que $\alpha^r \equiv 1 \pmod{N}$.

Por último, se calculan clásicamente dos factores de N a partir de α y r . Si r es impar o si $\alpha^{r/2} \equiv -1 \pmod{N}$ el algoritmo no ha sido capaz de encontrar un factor de N y es necesario probar con otro α . En otro caso, se cumple $(\alpha^r - 1) = (\alpha^{r/2} - 1)(\alpha^{r/2} + 1) \equiv 0 \pmod{N}$, por lo que N divide al producto $(\alpha^{r/2} - 1)(\alpha^{r/2} + 1)$. Por tanto, N tiene un factor común no trivial con $(\alpha^{r/2} - 1)$ y $(\alpha^{r/2} + 1)$ y los valores $\text{mcd}(\alpha^{r/2} - 1, N)$ y $\text{mcd}(\alpha^{r/2} + 1, N)$ son los factores de N que devuelve el algoritmo.

El cálculo cuántico del orden r es el núcleo del algoritmo de Shor. Para obtener r se busca el período de la función $f(x) = \alpha^x \pmod{N}$ aprovechando el principio de superposición cuántica: se construye un estado cuántico con todos los valores de x en $[0, N)$ y se evalúa $f(x)$ en todos ellos simultáneamente. Tras esta evaluación, se aplica la transformada cuántica de Fourier sobre el estado cuántico para obtener el orden r con alta probabilidad.

Nótese que el algoritmo de Shor es **probabilístico**. Podría no obtener factores de N si el α inicial no es coprimo con N , si el r calculado es impar o si cumple $\alpha^{r/2} \equiv -1 \pmod{N}$. También podría fallar si el ordenador cuántico en el que se ejecuta no se comportara idealmente (por falta de coherencia del estado cuántico durante el cálculo o error en la medida al aplicar la transformada de Fourier). En cualquier caso, la probabilidad de éxito de Shor es muy alta, por lo que llegaría a factorizar en tiempo polinómico aun cuando pudiera requerir varias iteraciones. Además, aplicando técnicas adicionales, puede llegar a garantizarse el éxito de Shor en una sola ejecución [84].

Desde el punto de vista práctico, a lo largo de los últimos 20 años se ha implementado el algoritmo de Shor en diversos sistemas cuánticos, demostrando su viabilidad y potencial. Sin embargo, las implementaciones hasta la fecha se han limitado a **pruebas de concepto** que abordaban la factorización de números pequeños. La realidad es que la computación cuántica aún no ha alcanzado la madurez suficiente para permitir a Shor resolver problemas de mayor tamaño, como se verá más adelante. A continuación, se presenta una tabla con los principales experimentos publicados:

Fecha	Factorización	Sistema cuántico
2001	$15=3 \cdot 5$	7 qubits basado en resonancia magnética nuclear [76].
2007	$15=3 \cdot 5$	4 qubits fotónicos [85].
2012	$15=3 \cdot 5$	4 qubits de estado sólido [86].
2012	$21=3 \cdot 7$	2 qubits fotónicos [87].
2015	$15=3 \cdot 5$	7 qubits en iones atrapados [88].
2019	$15=3 \cdot 5 / 21=3 \cdot 7 / 35=5 \cdot 7$	Procesador IBM usando 5 / 6 / 7 qubits superconductores [89].

Tabla 3-2. Implementaciones del algoritmo de Shor

3.4 El algoritmo de búsqueda de Grover

El otro algoritmo cuántico relevante desde el punto de vista de la seguridad criptográfica es el algoritmo que Lov K. Grover publicó en 1996 en su artículo "*A fast quantum mechanical algorithm for database search*" [90] para acelerar la **búsqueda** de un elemento dado en una secuencia de datos no ordenada.

El mejor algoritmo no cuántico para resolver este problema es la búsqueda lineal, ya que no es posible asumir ninguna estructura ni orden en la secuencia de entrada. En promedio es necesario evaluar la mitad de los elementos de la secuencia para conseguir probabilidad del 50% de encontrar el valor buscado, mientras que en el peor caso se han de evaluar todos los elementos de la secuencia. La búsqueda secuencial tiene por tanto complejidad $O(L)$, siendo L el tamaño de la secuencia o, dicho de otro modo, su tiempo de ejecución crece proporcionalmente al tamaño de la secuencia.

Por su parte, el algoritmo cuántico de **Grover** resuelve este problema en tiempo de ejecución $O(L^{1/2})$, lo que resulta en una **mejora cuadrática** respecto de la búsqueda secuencial clásica. Es interesante remarcar que, de hecho, se ha demostrado que este algoritmo resulta asintóticamente óptimo para el problema de búsqueda que resuelve, es decir, que no existe un algoritmo cuántico que pueda resolverlo con una complejidad menor que la de Grover [91]. Cabe observar que, aunque esta mejora es significativa, no resulta tan drástica como en el caso del algoritmo de Shor, que como se explicó reduce la complejidad de subexponencial a polinómica.

En el ámbito de la criptografía, el algoritmo cuántico de Grover podría aplicarse para reducir la complejidad de un ataque por **fuerza bruta** a un algoritmo de cifrado simétrico en un ordenador cuántico. Este tipo de ataque consiste en probar todas las claves posibles hasta encontrar la que se ha utilizado para cifrar algún mensaje. Si un algoritmo simétrico utiliza claves de n bits, el espacio de claves posibles tiene un tamaño de 2^n , por lo que el ataque de fuerza bruta clásico tiene una complejidad $O(2^n)$ mientras que el ataque de fuerza bruta cuántico tendría complejidad $O(2^{n/2})$.

De manera análoga, el algoritmo de Grover también tendría utilidad para encontrar **colisiones** de funciones hash de forma más eficiente en un ordenador cuántico. La resistencia a colisiones es una propiedad fundamental de este tipo de funciones, entendiéndose que una colisión consiste en encontrar dos valores distintos que tienen el mismo resumen. Si la salida de una función hash consiste en n bits, la búsqueda de colisiones clásica requiere un esfuerzo computacional de orden $O(2^n)$ mientras que su implementación cuántica vería reducida su complejidad a $O(2^{n/2})$ aprovechando la técnica de Grover.

Dado que la mejora cuántica proporcionada por el algoritmo de Grover es cuadrática y no exponencial, su impacto en la seguridad de los algoritmos criptográficos actuales es mucho menor que el de Shor. Siempre que se elijan longitudes de clave suficientemente grandes, tanto los algoritmos de cifrado simétrico como las funciones hash podrán resistir a los ordenadores cuánticos, a menos que estos algoritmos presenten una estructura particular que pueda llegar a ser explotada por los mismos.

El algoritmo de Grover, al igual que el de Shor, es un algoritmo cuántico **probabilístico** que utiliza la superposición de estados para realizar cálculos simultáneos y así reducir la complejidad del problema de búsqueda en la lista de L elementos. Grover comienza preparando un estado cuántico que representa todos los elementos de la lista en superposición. A continuación, aplica sobre este estado dos procesos que itera del orden de $O(L^{1/2})$ veces para aumentar la probabilidad de éxito: el señalamiento del estado objetivo y la amplificación de amplitudes.

Para señalar el estado objetivo, el algoritmo procesa el estado en superposición mediante un oráculo cuántico que realiza un cambio de fase en la amplitud del estado correcto, introduciendo un sesgo que permite diferenciarlo de los demás estados posibles. Tras la acción del oráculo, el algoritmo realiza una reflexión respecto al promedio de las amplitudes de todos los estados, que aumenta la amplitud del estado marcado y disminuye las amplitudes de los otros estados. Tras las sucesivas iteraciones de estos dos pasos, la medición final colapsa el estado cuántico recuperando el estado objetivo con muy alta probabilidad gracias a las sucesivas amplificaciones.

Al igual que ocurre con Shor, las implementaciones del algoritmo de Grover que se han llevado a cabo hasta ahora han empleado únicamente listas pequeñas (de a lo sumo 32 elementos) debido a la falta de madurez de la computación cuántica. Aunque estos **experimentos** son importantes para demostrar la viabilidad del algoritmo, aún distan mucho del orden de magnitud que podría desafiar la seguridad de los algoritmos de cifrado simétrico y las funciones hash. La Tabla 3-3 recopila las principales implementaciones de Grover publicadas hasta la fecha:

Fecha	Tamaño de lista	Sistema cuántico
2005	$2^2=4$	2 qubits en iones atrapados [92].
2017	$2^3=8$	2 qubits en iones atrapados [93].
2018	$2^4=16$	Procesador IBM usando 4 qubits superconductores [94].
2021	$2^4=16$	Procesador IBM usando 4 qubits superconductores [95].
2022	$2^5=32$	Procesador IBM usando 5 qubits superconductores e IonQ con 5 qubits en iones atrapados [96].
2024	$2^5=32$	Procesador IBM usando 5 qubits superconductores [97].

Tabla 3-3. Implementaciones del algoritmo de Grover

3.5 Hitos y desafíos de la computación cuántica

Dada la amenaza que supone la computación cuántica para la seguridad de los criptosistemas, es natural preguntarse cuál es el riesgo real al que se enfrentan. Hemos visto que existen algoritmos cuánticos capaces de comprometer dicha seguridad, como los de Shor o Grover, pero que a día de hoy los ordenadores cuánticos disponibles solo son capaces de abordar instancias básicas muy alejadas de la magnitud de los problemas que fundamentan la seguridad de los algoritmos criptográficos en uso actualmente. Esta afirmación puede comprobarse fácilmente atendiendo a las implementaciones de Shor y Grover hasta la fecha (en Tabla 3-2 y Tabla 3-3, respectivamente).

El desarrollo de **ordenadores cuánticos criptográficamente relevantes (CRQC**, por sus siglas en inglés) se enfrenta a dos retos tecnológicos fundamentales. El primero de ellos es la escalabilidad, es decir, la construcción de sistemas cuánticos que cuenten con un **número suficiente de qubits entrelazados** capaces de operar en estado superposición. En este sentido, se están empleando diferentes tecnologías para el desarrollo de qubits, siendo las más prominentes los qubits superconductores y los iones atrapados, aunque también se están explorando otras vías como el uso de puntos cuánticos o de átomos neutros [67] [68].

El segundo reto, estrechamente ligado con el anterior, consiste en mantener la **coherencia** de los qubits en estado de superposición el tiempo suficiente como para realizar las operaciones que precisan los algoritmos cuánticos, pues de otro modo se pierde la información que almacenan. La decoherencia de los qubits puede darse por su interacción con su entorno (variaciones de temperatura, campos electromagnéticos, vibraciones mecánicas, etc.), por interferencias con los demás qubits que componen el sistema e incluso por errores en las operaciones que se realizan sobre ellos [68].

Para mitigar tanto problemas de ruido cuántico, inherentes a los qubits, como de decoherencia, se están realizando avances en el desarrollo de técnicas de **corrección de errores** cuánticos. Estas técnicas tienen como objetivo agrupar varios qubits físicos (sensibles a la decoherencia) para formar un **qubit lógico** capaz de almacenar y conservar la información del estado cuántico en superposición sin verse afectado por la decoherencia de los qubits físicos individuales. La aplicación de estas técnicas de corrección puede llegar a estabilizar los ordenadores cuánticos que se están desarrollando, aunque limitando el número de qubits utilizables por los algoritmos cuánticos por la redundancia necesaria para la corrección de errores [98] [101].

Aunque hay muchos competidores en la carrera hacia la construcción de ordenadores cuánticos, en la última década las compañías estadounidenses IBM y Google han liderado la investigación y buena parte de los avances en este campo. Aunque no son los únicos actores relevantes en el sector, es interesante ver en qué situación se encuentran estos gigantes tecnológicos y cuáles son sus planes para los próximos años para entender el camino que queda por recorrer hasta la construcción de un CRCQ y valorar así el riesgo al que se enfrentan los criptosistemas actuales.

Lo primero reseñable es que tanto IBM como Google han apostado por desarrollar sus procesadores utilizando **qubits superconductores**, la tecnología más fácilmente escalable a día de hoy. Esta tecnología emplea materiales que conducen electricidad sin resistencia cuando su temperatura está próxima al cero absoluto (273 °C bajo cero). La manipulación de estos qubits se realiza mediante impulsos de microondas, que permiten cambiar sus estados de energía de forma muy precisa. Este tipo de qubits puede llegar a alcanzar tiempos de coherencia de microsegundos, suficiente para ejecutar algunos algoritmos cuánticos sencillos.

La Figura 3-3 muestra la hoja de ruta de **Google**, que incluye seis hitos tecnológicos en su camino hacia el desarrollo de ordenadores cuánticos con suficientes qubits como para que sea posible ejecutar programas relevantes [99]. En 2019 Google anunció la consecución del hito 1: logró supremacía cuántica al ejecutar en unos 200 segundos en un procesador cuántico una tarea computacionalmente intratable en ordenadores clásicos [100]. En 2023 anunció haber alcanzado el hito 2 tras lograr experimentalmente mejorar la corrección de errores manteniendo la coherencia de un sistema cuántico durante un periodo de tiempo más largo [101].

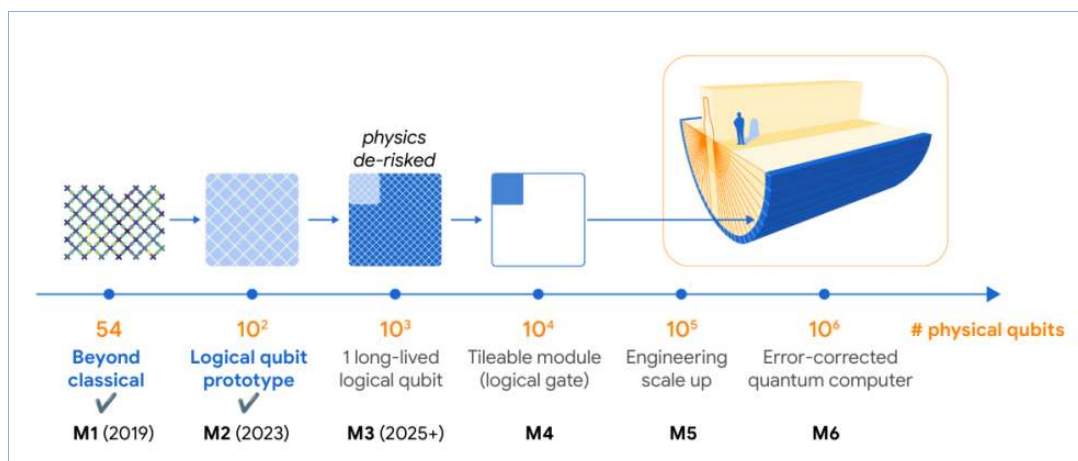


Figura 3-3 Hoja de ruta de Google hacia el ordenador cuántico [99]

El procesador cuántico más avanzado que tiene Google [102], al que ha llamado Willow, cuenta con 105 qubits superconductores y, según la compañía, representa un avance notable en su investigación porque ha logrado incrementar el número de qubits sin aumentar el nivel de error. Por otra parte, en un trabajo reciente [103], Google estimó que podría llegar a implementar un código corrector que lograra una tasa de error de 10^{-6} en un procesador de 1.457 qubits. Estos logros acercan a Google a su siguiente objetivo (para el que no tiene fecha prevista): disponer de un qubit lógico de larga duración, con a lo sumo 1 error cada millón de operaciones, utilizando para ello del orden de 1.000 qubits físicos.

La hoja de ruta de **IBM** se puede ver en la Figura 3-4 [104]. Se observa que la compañía ha apostado por alcanzar hitos anuales, enfocándose principalmente en aumentar progresivamente el número de qubits en sus procesadores, priorizando la escalabilidad de la tecnología a la mejora de la tasa de error. Además, IBM ha sido pionera en ofrecer desde el principio acceso a sus ordenadores cuánticos en un modelo de nube, universalizando el acceso a esta tecnología, y paralelamente ha desarrollado la herramienta Qiskit para simulación de algoritmos cuánticos.

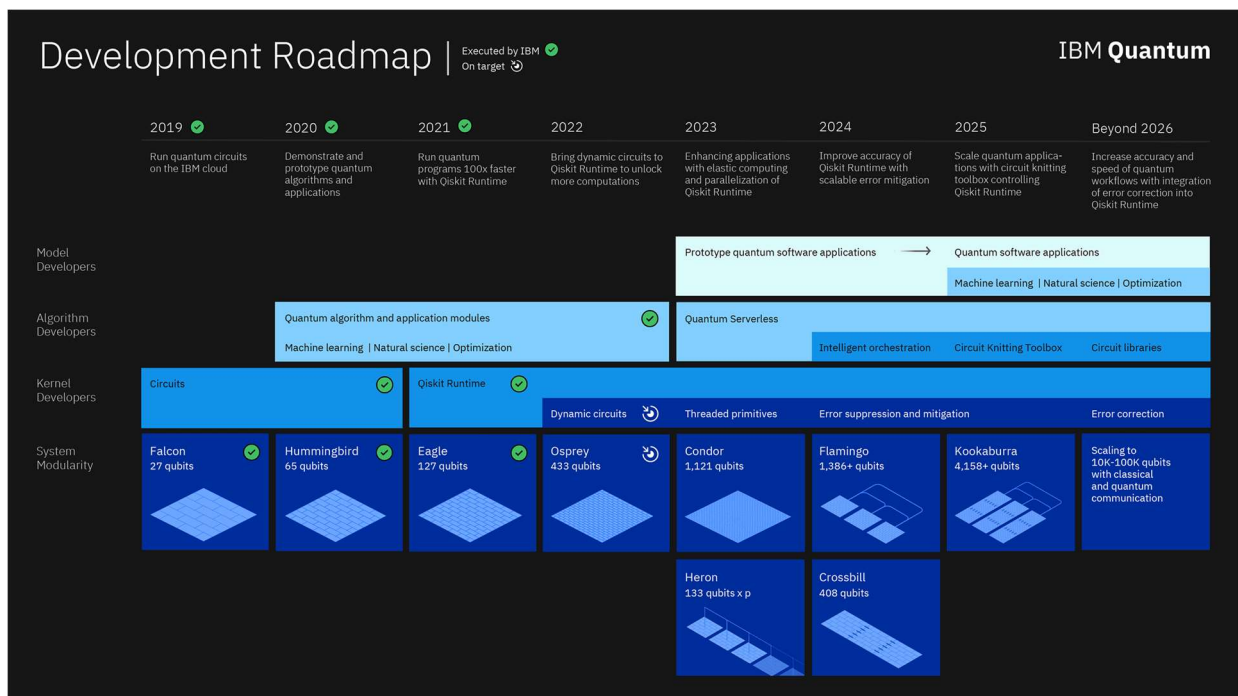


Figura 3-4 Hoja de ruta de IBM hacia el ordenador cuántico [104]

En 2023 IBM desarrolló los dos procesadores cuánticos que tenía previstos, Condor y Heron, diversificando su estrategia. Condor cuenta con 1.121 qubits superconductores, lo que representa un aumento del 50% en la densidad de qubits en comparación con el procesador anterior, situándolo a la vanguardia en términos de número de qubits alcanzados y reafirmando la apuesta de IBM por la escalabilidad en la computación cuántica [105]. Por otro lado, en el desarrollo de Heron la compañía ha priorizado la reducción de errores debidos al ruido cuántico y la interferencia entre qubits, con un enfoque orientado a la mejora del rendimiento y la fiabilidad en lugar de la escalabilidad. La versión de 2023 tenía 133 qubits superconductores, mientras que la de 2024 ha escalado hasta los 156 [106].

Como se puede ver, se están consiguiendo avances notables en computación cuántica, pero estos avances no son aún suficientes para alcanzar el ideal CRQC que pueda comprometer la seguridad de criptosistemas de clave pública basados en factorización o en logaritmos discretos. Tal y como concluye el excelente informe de prospectiva publicado por la Academia Nacional de las Ciencias estadounidense en 2019 [107], resulta altamente improbable que llegue a construirse un ordenador cuántico capaz de comprometer un módulo RSA de 2048 bits antes de 2030. Se profundiza sobre ello a continuación.

3.6 El camino hacia la factorización cuántica

La pregunta de cuántos qubits harían falta para lograr la factorización cuántica en un tiempo razonable de un módulo RSA de 2048 bits (**RSA-2048**) lleva años discutiéndose en la comunidad científica motivando la investigación en factorización cuántica. Se ha centrado la atención en esta longitud de clave porque su uso está muy extendido en la actualidad al considerarse suficientemente seguro desde el punto de vista clásico.

En 2012 la mejor estimación era que serían necesarios miles de millones de qubits para factorizar RSA-2048 [108], pero distintas optimizaciones del algoritmo de Shor lograron que esta estimación se redujera en 2021 hasta los 20 millones de qubits [109]. Resulta evidente que esta reducción de dos órdenes de magnitud supone un avance significativo hacia la realización de la factorización cuántica, pero también que aún dista mucho de ser alcanzable por los ordenadores cuánticos en desarrollo actualmente.

Desde 2021, la investigación en este campo ha llevado a la publicación de trabajos teóricos prometedores que reducen aún más el número de qubits necesarios con nuevas optimizaciones del algoritmo de Shor. Destaca el trabajo de Chevignard, Fouque y Schrottenloher de 2024 [110], que estima que podría llegar a factorizarse RSA-2048 en un ordenador cuántico con unos **1.700 qubits lógicos** (sin ruido ni errores). Este resultado supone reducir un orden de magnitud adicional el número de qubits necesarios respecto al resultado de 2021, si se tiene en cuenta la predicción de Google de emplear alrededor de 1.000 qubits físicos para implementar un qubit lógico.

Aunque este resultado reciente acerca el hito de alcanzar la factorización cuántica de RSA-2048, aún **parece lejano**. Cómo de cerca nos encontramos realmente de lograrlo va a depender, por un lado, de la evolución de la construcción de circuitos cuánticos que alojen suficientes qubits físicos y, por otro, de los avances en las técnicas de corrección de errores cuánticos. Este último punto es realmente significativo en vista de hallazgos como el reciente de Cai, que ha demostrado que la factorización con Shor de módulos RSA falla con muy alta probabilidad salvo que el nivel de ruido en el sistema cuántico sea insignificante para un subconjunto de números primos denso [111].

Es interesante revisar la encuesta que hace anualmente Michele Mosca para valorar el riesgo cuántico, en la que consulta a expertos relevantes de la academia y la industria [66]. En ella Mosca pregunta a los expertos cuán probable estiman que se construya en los próximos años un ordenador cuántico capaz de factorizar RSA-2048 en menos de un día. La previsión de los expertos que recoge el informe de 2023 se muestra en la Figura 3-5, en la que se observa que ven una posibilidad más bien baja de que la factorización cuántica ocurra en 10 años, y una **mayor probabilidad de que suceda en los próximos 15 a 20 años**.

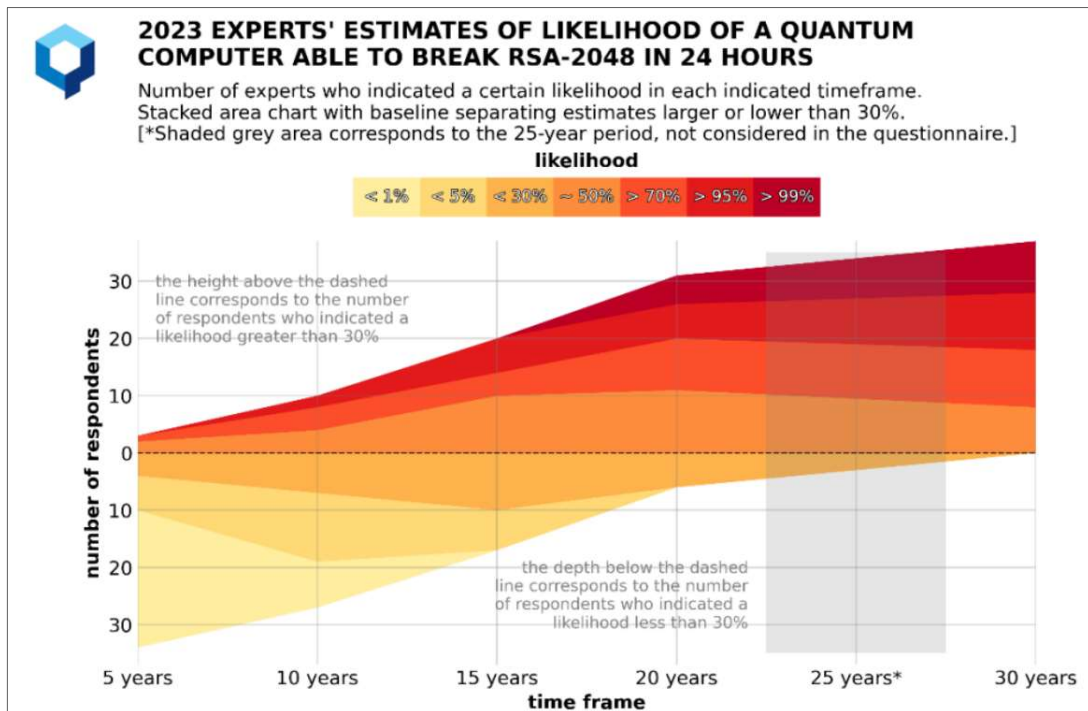


Figura 3-5 Estimación de expertos sobre la probabilidad de factorizar RSA-2048 [66]

Es relevante también hacer un ejercicio de retrospectiva y revisar la estimación que el propio Mosca realizó en 2015 ante el NIST, cuando pronosticó una probabilidad de que se lograra la factorización cuántica de RSA-2048 del 14% para 2026 y del 50% para 2031 [112]. Comparando estos valores con los del informe de 2023 que muestra la figura, se puede ver que, a pesar del importante desarrollo que ha tenido la computación cuántica desde 2015 a 2023, las expectativas de los expertos se han vuelto más conservadoras y la probabilidad se ha desplazado hacia el futuro.

Para finalizar conviene destacar que, aunque las estimaciones presentadas pueden considerarse razonables, se basan principalmente en el ritmo de evolución de las tecnologías cuánticas en los últimos años, por lo que, si se produjeran **avances inesperados** en alguno de los campos de investigación relacionados con la computación cuántica, podría acelerarse el desarrollo de un CRQC y en consecuencia acercar el hito de la factorización de RSA-2048. Entre las áreas que podrían experimentar mejoras significativas se encuentran la escalabilidad de los procesadores cuánticos, los esquemas de corrección de errores y el propio algoritmo de factorización [66] [107].

Del mismo modo, para asegurar que el avance de las tecnologías cuánticas no se ralentice y que las estimaciones sobre su desarrollo se mantengan vigentes, es esencial contar con una inversión sostenida a lo largo del tiempo. Hasta hoy, el desarrollo de estas tecnologías ha sido posible por una inversión elevada tanto del sector privado como de entidades gubernamentales. Sin embargo, hay preocupación en parte de la comunidad científica sobre la capacidad de las empresas para mantener este ritmo de inversión si no logran monetizar los ordenadores cuánticos disponibles actualmente, derivando en un estancamiento del desarrollo. Es por ello que se está potenciando la **investigación en problemas abordables con qubits ruidosos**, como simulación de sistemas físicos, optimización cuántica o aprendizaje automático [66] [107].

3.7 Resistencia frente a la amenaza cuántica

Aunque es muy poco probable que llegue a desarrollarse un CRQC en la próxima década, el riesgo que representa esta tecnología para la seguridad y la privacidad es tan alto que resulta fundamental que se tomen medidas preventivas cuanto antes. Es necesario, en primer lugar, **desarrollar alternativas** a los protocolos de cifrado basados en los algoritmos de clave pública actuales que sean capaces de resistir la computación cuántica que está por venir, para que el día que la amenaza cuántica se materialice el daño sea mínimo. Después, será necesario **estandarizar e implementar** estas alternativas, lo que implicará un tiempo de transición considerable [107].

Es importante enfatizar que no solo estará en riesgo la privacidad de la información que se cifre a partir de la puesta en funcionamiento del primer CRQC, sino que también los datos que están siendo cifrados actualmente serán vulnerables si un actor malicioso es capaz de interceptarlos y almacenarlos hasta entonces (ataque '**cosecha-ahora-descifra-después**'). La Figura 3-6 ilustra la ventana de oportunidad que tendría un atacante capaz de guardar datos cifrados hasta el desarrollo de un CRQC, enfatizando cuán urgente es abordar la transición [66]. Si la suma de: (i) tiempo necesario para la transición hacia soluciones resistentes a la amenaza cuántica, y (ii) tiempo que se pretende mantener la confidencialidad de la información, va más allá de la fecha en que se la amenaza cuántica se hará concreta, entonces habrá un periodo en el que la información será vulnerable.

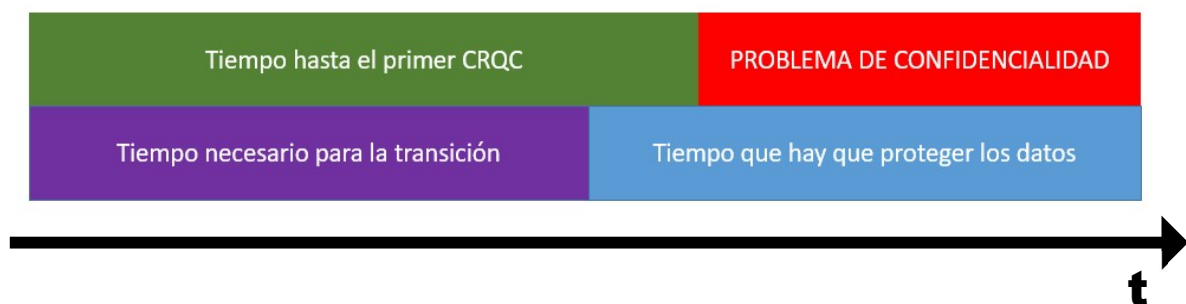


Figura 3-6 Ventana de oportunidad para el ataque 'cosecha-ahora-descifra-después' [66]

Afortunadamente, este proceso de transición ya ha empezado. La comunidad científica está investigando dos vías independientes para construir criptosistemas que incluyen el acuerdo de claves simétricas a través de un medio no confiable y que puedan **resistir** a la amenaza cuántica: la criptografía cuántica y la criptografía post-cuántica. Aunque ambos términos son muy similares, sus fundamentos son muy diferentes. El objetivo de la **criptografía cuántica** es desarrollar criptosistemas que aprovechen fenómenos cuánticos, mientras que el de la **criptografía post-cuántica** es desarrollar nuevos algoritmos que puedan ejecutarse en ordenadores clásicos y cuya seguridad no se vea comprometida por los ordenadores cuánticos.

Los orígenes de la criptografía cuántica se remontan a la década de 1970, cuando Stephen Wiesner compartió con Charles Bennett su revolucionaria idea de la codificación conjugada, que permitiría aplicar los principios de la mecánica cuántica para crear dinero no falsificable o para establecer un canal de transmisión cuántico [113]. Posteriormente, el propio Bennet y Gilles Brassard fueron perfeccionando este último punto hasta que, en 1984, presentaron su propuesta de utilizar un **canal cuántico** para transmitir de forma segura una clave secreta aleatoria, definiendo el protocolo BB84 que sentó las bases de la criptografía cuántica [114].

El mecanismo de intercambio de claves en un canal cuántico que describe BB84, denominado distribución cuántica de claves (**QKD**, *Quantum Key Distribution*), ha ido evolucionando desde entonces y existen implementaciones de transmisión fotónica en uso en la actualidad. La seguridad de QKD reside en el hecho de que cualquier intento de interceptar el canal cuántico por un observador malicioso altera el estado cuántico de los fotones, lo que permite a los comunicantes legítimos detectar dicha intervención y descartar los bits comprometidos. La clave aleatoria que se transmite de forma segura puede usarse para cifrar mensajes con algoritmos simétricos que no son vulnerables al algoritmo de Shor.

La criptografía cuántica en realidad no se limita a QKD, y cubre otras aplicaciones como la generación de números aleatorios y el desarrollo de protocolos cuánticos. Entre estos protocolos cabe destacar la computación cuántica segura multiparte, el cómputo cuántico delegado o los protocolos cuánticos de transferencia inconsciente [115]. Existen ya generadores aleatorios comerciales (QRNG) que aprovechan la naturaleza intrínsecamente aleatoria de determinados fenómenos cuánticos, que se emplean, por ejemplo, para generar las claves de los sistemas QKD que ya están en uso. Sin embargo, el desarrollo de los protocolos cuánticos se mantiene aún a un nivel teórico y experimental, y no se han implementado aplicaciones prácticas en el mundo real.

A pesar de que QKD es una tecnología muy útil para comunicar dos nodos de forma segura, presenta importantes **limitaciones**. Desde un punto de vista operativo, QKD requiere dispositivos cuánticos específicos para la transmisión y recepción de la señal fotónica. Desde un punto de vista técnico, aún no ha sido posible resolver algunos problemas fundamentales para explotar QKD a gran escala. Uno de estos problemas es que la señal fotónica transmitida, ya sea a través del espacio libre o por fibra óptica, sufre una atenuación que no se puede corregir, pues la propia naturaleza cuántica de los fotones impide que puedan copiarse o amplificarse. Esta atenuación limita la distancia efectiva a la que pueden encontrarse los nodos y dificulta la escalabilidad de QKD [116].

En este sentido juega un papel crucial el desarrollo de repetidores cuánticos, que sean capaces de trasladar los estados cuánticos de un sistema a otro y extender así las señales distancias más largas. Estos repetidores permitirían interconectar diferentes sistemas QKD y llegar a construir infraestructuras de red cuántica más extensas y complejas, acercando el ideal de un Internet cuántico sobre el que todo el mundo podría a priori comunicarse de forma segura [116] [117]. En la sección 4 se profundiza en el tema de las comunicaciones cuánticas y su utilidad para garantizar la privacidad de las comunicaciones frente a un CRQC.

La otra aproximación para resistir a la amenaza cuántica es la llamada criptografía post-cuántica (**PQC**, por sus siglas en inglés), también conocida como criptografía resistente a la computación cuántica, denominación que resulta bastante más precisa. A diferencia de la criptografía cuántica, la post-cuántica no aprovecha fenómenos cuánticos ni necesita dispositivos cuánticos específicos, sino que consiste en algoritmos criptográficos para hardware convencional que pueden emplearse como alternativa a los algoritmos vulnerables con un CRQC, principalmente de clave pública [65].

Tras la publicación del algoritmo de Shor en 1994, la comunidad criptográfica comenzó a buscar problemas matemáticos que pudieran resultar intratables tanto para los ordenadores clásicos como para un hipotético ordenador cuántico universal. La búsqueda de alternativas a los problemas de factorización entera y de cálculo del logaritmo discreto, débiles frente al algoritmo de Shor en un CRQC, se intensificó en la década de los 2000, y fue precisamente en esta época en la que la denominación de criptografía post-cuántica se popularizó en la literatura académica [118].

La investigación en este campo fue impulsada por el NIST con la publicación en 2016 del concurso para definir estándares de PQC [65]. Las **matemáticas** en las que se han basado los numerosos algoritmos criptográficos presentados a este concurso son diversas: aprendizaje con errores en retículos, códigos de corrección de errores, solución de sistemas de polinomios multivariantes, firmas digitales basadas en hashes e isogenias de curvas elípticas. Recientemente, en agosto de 2024, el NIST estandarizó los tres primeros algoritmos seleccionados en el concurso [119], y dejó abierta la posibilidad de publicar nuevos estándares en los próximos años para abarcar más casos de uso. Se profundizará sobre criptografía post-cuántica en la sección 5.

4 COMUNICACIONES CUÁNTICAS

En la sección anterior se presentó la criptografía cuántica como una de las posibles soluciones para crear criptosistemas capaces de resistir la amenaza cuántica, aprovechando fenómenos cuánticos para evitar el uso de algoritmos de clave pública vulnerables ante un CRQC. En esta sección, se aborda la distribución cuántica de claves (comúnmente conocida como QKD, por sus siglas en inglés), un método que permite a dos partes acordar una clave transmitida a través de un canal cuántico. QKD es actualmente la rama más avanzada de la criptografía cuántica, existen multitud de productos comerciales y varias redes implementadas como prueba de concepto.

Se explica como QKD, que desde un punto de vista teórico es incondicionalmente segura, puede tener vulnerabilidades cuando se implementa en la práctica. Además, aunque las propiedades físicas de QKD son útiles para detectar intrusos en el canal cuántico, estas propiedades hacen que los sistemas QKD sean vulnerables a ataques de denegación de servicio, impactando negativamente en su disponibilidad. Por otro lado, los sistemas QKD requieren un canal auxiliar no cuántico para garantizar que las partes acuerden la misma clave, en el que la autenticación mutua es esencial para evitar ataques activos que puedan comprometer su seguridad.

En esta sección también se analizan las limitaciones de QKD, que dificultan su adopción masiva como solución a la amenaza cuántica. Además de la necesidad de equipos e infraestructura costosos y complejos, la naturaleza cuántica del enlace limita tanto la distancia de transmisión como la tasa de generación de claves. Para superar estas limitaciones, se están desarrollando infraestructuras de comunicaciones cuánticas con repetidores intermedios que facilitan la conexión de nodos QKD. Estas infraestructuras, tanto terrestres como satelitales, buscan ampliar el alcance y la eficiencia de QKD en el camino hacia el ideal de un Internet cuántico.

Para concluir, se examina como varias agencias de seguridad de reconocido prestigio han desaconsejado el uso de QKD como solución para la amenaza cuántica, favoreciendo en su lugar la criptografía post-cuántica, al considerarla una opción más madura y que permite una transición más sencilla al aprovechar las infraestructuras de comunicación existentes.

4.1 Distribución cuántica de claves

La **distribución cuántica de claves** es actualmente la rama más desarrollada de la criptografía cuántica y uno de los mecanismos que se están adoptando para construir criptosistemas resistentes a la amenaza cuántica. Desde la publicación en 1984 del protocolo BB84, la tecnología ha evolucionado considerablemente y hoy en día existen numerosos productos comerciales y sistemas de QKD implementados por todo el mundo.

QKD consiste básicamente en un **establecimiento de clave entre dos partes por transporte**. Una de las partes genera una clave aleatoria (o pseudo-aleatoria) y la comparte con la otra utilizando un canal de transmisión cuántico. La ventaja que ofrece QKD radica en que, gracias a las propiedades cuánticas del canal de transmisión, ningún actor malicioso con capacidad de observarlo puede recuperar la clave transmitida. Por un lado, el teorema de no clonación garantiza que un adversario no puede hacer una copia del flujo de datos sin alterarlo. Por otro, los comunicantes legítimos pueden detectar la intromisión en el canal cuántico y actuar descartando los bits comprometidos, ya que por el principio de incertidumbre de Heisenberg cualquier medición altera el estado del sistema cuántico [114] [120].

Tras este proceso de transmisión cuántica de bits, los comunicantes pueden utilizar la secuencia aleatoria enviada como clave para cifrar mensajes utilizando algoritmos simétricos y, posteriormente, transmitir los mensajes cifrados por un canal clásico, evitando la necesidad de usar algoritmos de clave pública potencialmente vulnerables a la computación cuántica. Idealmente, si la tasa de transmisión del canal cuántico resultara suficiente, los comunicantes podrían llegar a usar las claves transmitidas para cifrar con *One Time Pad*, alcanzando así la **seguridad incondicional** que Claude Shannon definió en los fundamentos de la teoría de la información [46].

Con respecto a la aleatoriedad de la clave, es habitual que los sistemas de QKD utilicen **generadores cuánticos de números aleatorios** (QRNG, *Quantum Random Number Generator*), aunque no es imprescindible y sería suficiente emplear generadores pseudo-aleatorios adecuados para criptografía, como los que se utilizan habitualmente para generar claves en redes de comunicaciones clásicas. Existen diferentes alternativas para construir QRNG, todas ellas aprovechando la naturaleza probabilística intrínseca de la física cuántica, así como varios QRNG comercializados [121]. A lo largo de esta sección se asumirá que la clave aleatoria intercambiada es apropiada para usos criptográficos, con independencia del generador utilizado.

Aunque cabe la posibilidad de utilizar diferentes sistemas cuánticos para establecer el canal de transmisión de claves, los **sistemas fotónicos** son de lejos la opción más extendida y, de hecho, la única disponible comercialmente [122]. La alternativa más prometedora al uso de fotones para QKD es la construcción de sistemas cuánticos con iones atrapados, aunque esta tecnología aún se encuentra en fase experimental [123]. Los fotones son idóneos para transmisión en el espacio libre, al verse menos afectados que otras partículas por fuentes de ruido ambiental como la radiación electromagnética, pero tienen además la ventaja de que pueden transmitirse a través de fibras ópticas. Además, las tecnologías para generar, manipular y detectar fotones se encuentran muy desarrolladas en la actualidad, por lo que la implementación práctica de QKD usando fotones resulta abordable [122] [124].

Según el tipo de codificación de la información, los protocolos de QKD se dividen en dos categorías, protocolos de **variable discreta** (DV, *Discrete Variable*) y de **variable continua** (CV, *Continuous Variable*). En DV-QKD los fotones se transmiten individualmente y la información se codifica en modos ópticos discretos de cada fotón, como la polarización o los intervalos de tiempo. Por otro lado, en CV-QKD la información se codifica utilizando variables continuas del campo electromagnético, como la amplitud y la fase de los estados de luz, en lugar de en estados discretos de fotones individuales como ocurre en DV-QKD [125].

Mientras que la **industria de DV-QKD** ha alcanzado ya un nivel de madurez aceptable, con numerosos productos comerciales y sistemas en operación que implementan protocolos de este tipo desde hace años, CV-QKD aún se encuentra en fase de desarrollo y de pruebas de concepto. La compañía suiza ID Quantique [126], la estadounidense MagiQ Technologies [127], la china QuantumCTek [128] y la británica Toshiba Research Europe [129] lideran el desarrollo y la comercialización de productos DV-QKD, aunque hay muchas otras compañías que también ofrecen este tipo de productos.

En la actualidad hay mucha **investigación en CV-QKD** sobre fibra óptica, ya que su uso permitiría, a priori, alcanzar distancias más largas en los enlaces y conseguir mejores tasas de generación de claves [130]. De hecho algunas compañías, como la española LuxQuanta [131], ya comercializan equipos CV-QKD. Sin embargo, hasta la fecha no se ha logrado que el alcance de enlaces tipo CV-QKD supere al de DV-QKD, aunque se siguen produciendo avances en esta línea [132]. El desarrollo de CV-QKD podría reducir considerablemente el coste de los enlaces por fibra, no solo porque permiten usar la infraestructura de fibra existente (no dedicada) de los operadores de telecomunicaciones, sino también porque se emplean láseres comerciales y detectores homodinos, mucho más económicos que el equipamiento específico que requiere DV-QKD.

4.2 Distribución cuántica de claves discreta

DV-QKD, la aproximación clásica a QKD, es la más utilizada en la actualidad. Los protocolos DV-QKD utilizan estados discretos de los fotones para codificar los bits de la clave aleatoria que se intercambia, de manera que cada fotón representa un único bit. Lo más habitual es que **los bits se codifiquen en la polarización de los fotones**, como ocurre en el protocolo primigenio BB84 [114] o en sus variantes SARG04 de 2004 [133], que mejora la resistencia de BB84 frente a ciertos ataques, o protocolo de 6-estados de 1998 [134], con una mejor detección de errores.

Es interesante revisar el protocolo **BB84**, cuyo funcionamiento se representa gráficamente en la Figura 4-1. Para comenzar, el emisor (Alice) elige dos secuencias de bits aleatorias, $\{k_i\}$ y $\{\alpha_i\}$, la primera corresponde con la clave a transmitir y la segunda con la elección de base de polarización con la que va a codificar los bits de clave. En función de cada bit α_i , Alice utiliza la base rectilínea $\oplus = \{0^\circ, 90^\circ\}$ o bien la base diagonal $\otimes = \{45^\circ, -45^\circ\}$ para codificar el bit k_i en la polarización del fotón, y después lo envía por el canal cuántico. La elección de estas bases no es causal: los estados en cada una de ellas son ortogonales entre sí y, además, las propias bases son ortogonales entre sí. En el otro extremo, el receptor (Bob) genera otra secuencia aleatoria $\{\beta_i\}$ para elegir con qué base, $\oplus$ o $\otimes$, va a medir cada uno de los fotones que recibe [114] [135].

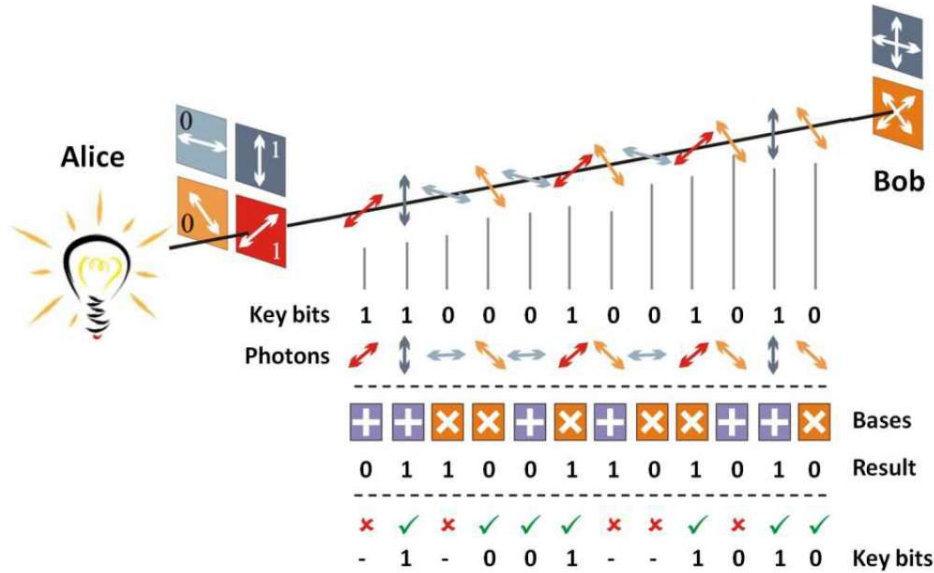


Figura 4-1 Esquema del protocolo BB84 para DV-QKD [135].

Cuando se completa la transmisión de la secuencia de fotones, comienza la fase conocida como **discusión pública**. En esta fase, Alice y Bob intercambian las bases que utilizaron a través de un canal auxiliar no cuántico, de forma que ambos pueden comprobar si las polarizaciones usadas para codificar y para medir coinciden ($\alpha_i = \beta_i$) y pueden conservar el bit de clave k_i o si, por el contrario, no coinciden y han de descartarlo. Dado que ambos eligieron las bases de forma aleatoria, coincidirán aproximadamente la mitad de las veces, por lo que la clave efectiva quedará reducida. Durante la discusión pública los comunicantes solo necesitan informarse mutuamente de las bases utilizadas, pero no se transmiten los bits de clave.

Cabe preguntarse qué ocurre cuando un actor malicioso (Eve) trata de interceptar en el canal cuántico. En este caso, Eve debe elegir una base de polarización para medir y recuperar cada bit codificado. Gracias a la ortogonalidad, cuando un fotón se mide en una base diferente a la que se usó para prepararlo el resultado es aleatorio, por lo que Eve solo tiene un 50% de probabilidad de elegir la base correcta y recuperar el bit original. Ahora bien, al medir Eve cambia el estado cuántico del fotón observado y esto causará que el bit que descodifica Bob sea incorrecto el 25% de las veces (Bob asume la elección α_i de Alice, pero la polarización podría haberse alterado tras la medida de Eve).

Para detectar la presencia de Eve, Alice y Bob realizan una **comprobación de errores** a través del canal auxiliar, comparando una fracción de los bits de clave acordados, para lo que suelen emplearse códigos correctores. Esta comprobación introduce una reducción adicional en la clave efectiva. En el último paso del BB84, los comunicantes realizan dos procesos: la **reconciliación de información**, en el que eliminan las discrepancias en sus respectivas secuencias de bits de clave y, la **ampliación de la privacidad**, en el que transforman los bits de clave efectiva restantes en una nueva secuencia aleatoria (normalmente mediante funciones hash por su no invertibilidad), protegiéndose así contra la posibilidad de que Eve haya recuperado algunos bits [114] [122] [136].

Además de BB84, existen protocolos alternativos de DV-QKD que también emplean la polarización como medio para codificar la información, pero que se basan en la transmisión de pares de fotones entrelazados y en la correlación entre sus estados, como el **E91** ideado por Artur Ekert en 1991 [137], y el **BBM92** desarrollado por Bennett, Brassard y Mermin en 1992 [138]. Sin embargo, estos protocolos aún no han llegado a trascender el plano experimental debido a la dificultad práctica de generar y mantener estados de entrelazamiento estables a largas distancias y a la complejidad técnica que conlleva su implementación.

Por otro lado, hay protocolos DV-QKD que no utilizan la polarización para codificar información, sino otros estados discretos. Cabe destacar **DPS** (*Differential Phase Shift*), de 2002, que se basa en el envío de pulsos sucesivos de luz y codifica los bits en la diferencia de fase entre pulsos sucesivos, resultando más robusto que BB84 y sus variantes frente a algunos ataques [139]. También **COW** (*Coherent One Way*), de 2007, que se basa en el envío de pulsos coherentes de luz y codifica los bits en función de la presencia o ausencia de fotones en dichos pulsos [140]. Aunque BB84 sigue siendo el protocolo más utilizado, también existen aplicaciones prácticas tanto con DPS como con COW (sobre todo con el primero), que tienen la ventaja de no requerir a las partes una selección de bases y que logran un alcance algo mayor [126] [127].

También es relevante destacar que existen otros protocolos de DV-QKD que, aun suponiendo avances significativos a nivel teórico respecto a los usados en la actualidad, aún no se han desarrollado lo suficiente y se encuentran en una etapa experimental. Entre los más destacados están: **KMB09**, que emplea técnicas avanzadas de corrección de errores para reducir el impacto del ruido [141]; **T12**, que utiliza pulsos ópticos modulados para codificar la información de manera eficiente, aumentando la tasa de generación de claves [142]; y **HDQKD**, que codifica varios bits por fotón en estados de alta dimensionalidad para mejorar la tasa de generación [143].

Para concluir, es importante destacar que todos los protocolos de DV-QKD requieren un **canal auxiliar no cuántico** (público) para realizar la corrección de errores y garantizar que los comunicantes alcancen la misma clave secreta. Estos errores pueden introducirlos cualquier observador del canal cuántico, pero también pueden deberse a imperfecciones del propio canal: interferencias ambientales, pérdida de fotones, decoherencia de su estado cuántico, ruido en los fotodetectores, etc. En la fase de corrección, los comunicantes evalúan la tasa de errores y descartan la clave intercambiada si está por encima de un umbral establecido. La autenticación mutua en este canal auxiliar clásico es fundamental para la seguridad de los sistemas DV-QKD, como se verá en lo que sigue.

4.3 Limitaciones de la distribución cuántica de claves

A pesar del potencial de QKD para garantizar resistencia cuántica, esta tecnología tiene varias limitaciones que dificultan su escalabilidad y complican su adopción masiva. La mayoría de estas limitaciones tienen que ver con la propia **naturaleza** de los sistemas cuánticos y con los desafíos técnicos que tiene su **implementación**. En la actualidad los investigadores están desarrollando algunas tecnologías que podrían mitigar algunas de estas limitaciones, como los repetidores cuánticos, las memorias cuánticas y la teleportación cuántica, pero estos desarrollos aún no están lo suficientemente maduros para su aplicación práctica [124] [125].

El primer problema que presenta QKD es la **limitada distancia a la que se pueden establecer enlaces** debido a la atenuación de la señal fotónica. Tanto en las fibras ópticas como en los enlaces de espacio libre, los fotones pierden intensidad debido a diversos factores, como la absorción en el material y la dispersión en el canal. No es físicamente posible amplificar la señal, pues se alteraría el estado de los fotones. En fibras ópticas, la atenuación aumenta significativamente a medida que la distancia se extiende, limitando la transmisión a unos pocos cientos de kilómetros antes de que los fotones se pierdan o se debiliten tanto que no puedan ser detectados de manera confiable. En espacio libre la atenuación es menor, pero los fenómenos atmosféricos afectan la transmisión [122] [124] [135].

Otra limitación importante es la **reducida tasa de generación de claves**, especialmente en el caso de DV-QKD, dado que en este tipo de protocolos los fotones se preparan y transmiten individualmente, por lo que hace que las tasas de emisión suelen ser bajas. Además, la atenuación del canal no solo afecta a la distancia alcanzable en un enlace, sino que también impacta negativamente en la tasa de generación de claves. A medida que aumenta la distancia, una menor cantidad de fotones logra alcanzar el fotodetector, lo que reduce la cantidad de bits de clave que se pueden recuperar (en la práctica, la tasa disminuye exponencialmente con la distancia de transmisión). Por último, esta tasa también se ve afectada por el tiempo necesario para el post-procesado de los bits enviados que los comunicantes llevan a cabo en el canal auxiliar no cuántico [114] [124].

En la práctica, los enlaces por fibra óptica con productos comerciales de DV-QKD pueden alcanzar distancias entre 50 y 150 km, con tasas de transmisión que oscilan entre 1 kbps y 1 Mbps [126] [127] [129] [128]. Los equipos de CV-QKD, aunque potencialmente pueden llegar a lograr mayores alcances, en la actualidad solo alcanzan distancias entre 20 y 100 km con tasas de transmisión generalmente más altas, que van de 100 kbps a 10 Mbps, pudiendo ser algo mayores en distancias de unos pocos kilómetros. La atenuación en fibra óptica dedicada es típicamente 0,2 dB/km, mientras que si la fibra es compartida aumenta hasta 0,3-0,4 dB/km por las interferencias y el mayor nivel de ruido [130] [131] [132].

Por otra parte, la atenuación de la luz es alta a altitudes bajas pero despreciable en el vacío por encima de la atmósfera terrestre. Los enlaces cuánticos de espacio libre terrestres no son prácticos al ser susceptibles a obstáculos en la línea de visión, a atenuaciones fuertes por las condiciones climáticas e incluso a los efectos de la curvatura de la Tierra. Sin embargo, los enlaces cuánticos satelitales pueden aprovechar la ventaja de la escasa atenuación fuera de la atmósfera, donde apenas hay absorción ni decoherencia, y alcanzar distancias mucho mayores que los enlaces de fibra óptica. Se puede observar en la Figura 4-2, que compara la atenuación estándar de la fibra con la del espacio libre (según parámetros del enlace con el satélite Micius [144]), como ésta última es más ventajosa en distancias superiores a los 70 - 100 km. Se profundiza en QKD satelital en la sección 4.5.

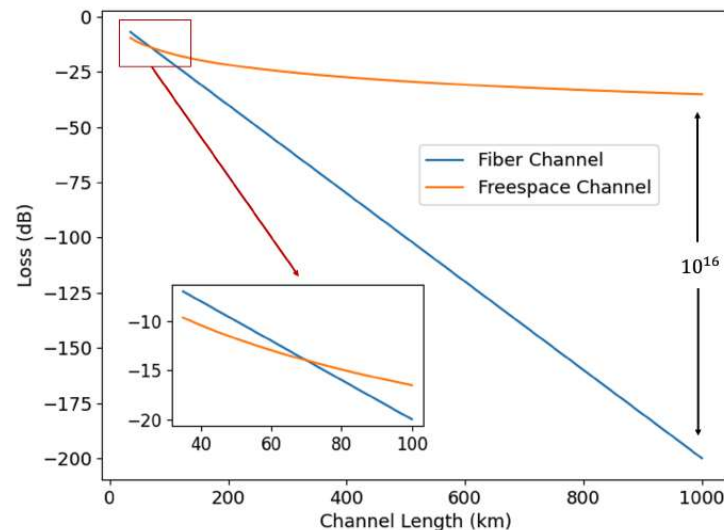


Figura 4-2 Pérdidas típicas por atenuación en enlaces de fibra óptica y de espacio libre [144].

La **necesidad de autenticación en este canal auxiliar** supone otra importante limitación de los protocolos QKD. Este canal es fundamental para realizar la discusión pública, la corrección de errores, la reconciliación de información y la ampliación de la privacidad. Aunque el canal puede ser público, ya que los bits de clave no se transmiten por él, los comunicantes deben autenticarse para prevenir ataques de hombre en el medio que puedan comprometer la seguridad [145], para lo que pueden emplear bien secretos pre-compartidos o bien esquemas de firma basados en algoritmos de clave pública. La dependencia de este canal clásico autenticado representa uno de los aspectos más controvertidos de la tecnología QKD, como se discutirá más adelante [114] [122] [125].

Desde el punto de vista de la implementación, también es un factor limitante el hecho de que el despliegue de enlaces DV-QKD necesite **equipos complejos y costosos**, como son las fuentes de fotones individuales y los fotodetectores de alta precisión. Además, la operatividad de estos sistemas se ve dificultada por la necesidad de **canales de transmisión dedicados**, especialmente cuando se requiere el despliegue de fibras ópticas de alta calidad dedicadas o enlaces satelitales en el espacio libre (en este caso los costes son enormes, pues la infraestructura espacial y la alineación precisa necesarias añaden gran complejidad) [124] [125]. El desarrollo de sistemas CV-QKD podría mitigar en buena medida este problema, dado que permitiría el uso de equipamiento de propósito general para generar y detectar fotones, así como el empleo de fibras ópticas no dedicadas [130].

4.4 Seguridad de la distribución cuántica de claves

La principal ventaja que ofrece QKD es su **seguridad incondicional**, que está garantizada desde el punto de vista de la teoría de la información y basada en las leyes fundamentales de la física cuántica. Esta seguridad ha sido demostrada teóricamente frente a cualquier adversario, con independencia de los recursos computacionales de los que disponga, ya sean superordenadores clásicos o los futuros ordenadores cuánticos [146] [147] [148] [125]. Las demostraciones de seguridad formales asumen que las claves transmitidas son aleatorias y que se emplean posteriormente para cifrar simétricamente con el cifrado perfecto OTP (*One Time Pad*).

Desde el punto de vista formal, QKD mejora a los algoritmos de clave pública, tanto los clásicos como los post-cuánticos, puesto que la seguridad de estos algoritmos depende de la intratabilidad de resolver determinados problemas matemáticos que podrían llegar a ser vulnerados en algún momento debido a mejoras en los algoritmos o en la capacidad computacional. Además, los sistemas QKD garantizan **resistencia cuántica** y la información protegida con claves transmitidas por este tipo de sistemas es capaz de resistir al ataque ‘cosecha-ahora-descifra-después’, al contrario de lo que ocurre con los algoritmos de clave pública clásicos.

Ahora bien, aunque QKD es teóricamente seguro, en la práctica se enfrenta a **vulnerabilidades en sus implementaciones**, normalmente debidas a imperfecciones de los dispositivos. Si un actor malicioso puede acceder físicamente a los dispositivos de codificación y decodificación de un sistema QKD podría llegar a comprometer su seguridad, pero incluso es posible que pueda llegar a atacar al sistema sin necesidad de este acceso físico, tan solo interaccionando con los dispositivos a través del propio canal de transmisión [122] [125] [149]. Durante las últimas dos décadas la comunidad ha estado trabajando en contramedidas para evitar las vulnerabilidades que se han ido encontrando, tanto mejorando la robustez de los equipos como adaptando los protocolos, pero la amenaza sigue existiendo.

La tipología de ataque más habitual a QKD son los **ataques de canal lateral**, en los que un adversario aprovecha fugas de información no intencionadas en los dispositivos para obtener una ventaja que le permita vulnerar la seguridad del protocolo QKD sin llegar a ser detectado. Los ejemplos más representativos de este tipo de ataques son el de división del número de fotones [150], el de desplazamiento de tiempo [151] [152], el de caballo de troya [153] y el de luz brillante [154] [155], que se revisan a continuación. Estos cuatro no son los únicos ataques de canal lateral sobre dispositivos QKD; pueden verse otros en el informe dedicado de ETSI [149] y en las publicaciones de los autores de estos ataques, ya que siguen investigando activamente en este campo.

El **ataque de división del número de fotones** aprovecha que los sistemas DV-QKD utilizan láseres atenuados como fuente de generación de fotones individuales. El número de fotones que genera el láser sigue una distribución de Poisson, y se ajusta la intensidad del láser para que la mayoría de las veces genere un único fotón o ninguno, pero no es viable evitar que en ocasiones emita 2 o más fotones. Cuando el láser genera más de un fotón, el adversario puede captar uno de ellos y dejar circular los demás por el canal cuántico, sin afectar a la comunicación entre las partes y sin ser detectado, dado que no mide directamente en dicho canal. Si el adversario puede almacenar los fotones detectados y, posteriormente, intercepta en el canal auxiliar la base del emisor, podrá recuperar los bits codificados en dichos fotones. La contramedida habitual para evitar este tipo de ataque es el uso de estados señuelo [156], que mediante variaciones en la intensidad del láser permite detectar este ataque.

Por otra parte, el **ataque de desplazamiento de tiempo** aprovecha que los sistemas DV-QKD típicamente utilizan dos fotodetectores diferentes para identificar los bits 0 y 1. Estos detectores se activan en ventanas de tiempo específicas según el tiempo esperado de llegada de los fotones individuales. Un adversario puede llegar a desfasar el tiempo de llegada de los fotones (adelantándolos o retrasándolos) mediante conmutadores ópticos de alta velocidad, y aprovechar la ineficiencia de los detectores en determinadas ventanas temporales para conseguir que uno de ellos tenga mayor probabilidad de detectar el fotón. De esta forma, el adversario puede llegar a controlar qué bit se detecta con mayor probabilidad, sin generar errores que alerten a los comunicantes legítimos. La contramedida habitual contra este tipo de ataque consiste en una calibración más precisa de los detectores para alinear mejor sus ventanas de detección.

El **ataque de caballo de troya** aprovecha que los emisores de fotones en los sistemas QKD son dispositivos ópticos que pueden reflejar una pequeña cantidad de luz. Un adversario puede lanzar pulsos de luz hacia el emisor fotónico y captar los fotones reflejados a través del canal cuántico. La luz reflejada puede revelar detalles sobre los componentes internos del dispositivo y sobre su configuración, como por ejemplo los ajustes del modulador de polarización o fase que se utiliza para codificar los bits o, incluso, el estado del modulador a partir del cual es posible inferir la base que utiliza el emisor y en algunos casos hasta los bits que se transmiten. Las contramedidas más comunes contra este ataque son el uso de aisladores ópticos para prevenir la entrada de pulsos brillantes y la monitorización pasiva de la luz entrante en el emisor.

Otro ataque de canal lateral es el **ataque de luz brillante**, en el cual un adversario utiliza una fuente de luz clásica brillante, típicamente un láser, para inundar el detector del sistema DV-QKD e interferir con la detección de los fotones que se transmiten en la comunicación cuántica entre las partes. Esta iluminación malintencionada le permite al adversario influir en el comportamiento del detector y, mediante sucesivos ajustes de su intensidad, llegar a controlar los resultados que produce con una probabilidad alta y deducir información sobre la clave transmitida. La publicación en 2010 de este ataque tuvo un impacto notable, pues pudieron recuperarse claves transmitidas con equipos comerciales de QKD de forma inadvertida [154]. De nuevo, las contramedidas propuestas para mitigar el riesgo de este tipo de ataques son de índole físico: mejoras en la optoelectrónica de los detectores y en las condiciones operativas para minimizar la interferencia externa.

Los problemas de seguridad derivados de las implementaciones de QKD no son los únicos que afectan a esta tecnología. Otra potencial vulnerabilidad de QKD podría producirse si se empleara algún mecanismo de **autenticación débil en el canal auxiliar**, pues al ser este canal público y no cuántico sería posible que un adversario llegara a suplantar a alguno de los comunicantes legítimos mediante un ataque de hombre en el medio [145] [125]. Si las partes no comparten inicialmente un secreto para la autenticación, lo natural es que utilicen firmas digitales, y si se pretende que estas firmas resistan a la amenaza cuántica, deben basarse en algoritmos de clave pública post-cuánticos como los que se introducirán en la siguiente sección. Nótese que la necesidad de esta autenticación en el canal auxiliar podría limitarse a la primera sesión entre los comunicantes, ya que posteriormente podrían parte de las claves transmitidas cuánticamente como secreto en común [120] [122] [125].

Por último, es importante destacar que los protocolos QKD son susceptibles a ataques de **denegación de servicio** (DoS, *Denial of Service*) [157]. Como se vio al revisar el protocolo BB84, un adversario que intercepte fotones en el canal cuántico va a alterar su estado, introduciendo errores que los comunicantes pueden detectar en el post-procesado que realizan sobre el canal auxiliar. Si estos errores son numerosos, lo que ocurrirá si la interceptación del canal es continuada, superarán el umbral definido por las partes y no llegará a acordarse una clave. Esta debilidad es inherente a la tecnología, por lo que tiene difícil solución y puede llegar a limitar el uso de sistemas QKD en escenarios en los que la disponibilidad tenga que estar garantizada. Para mitigar el impacto en disponibilidad de los ataques DoS, se precisa de enlaces alternativos por los que poder redirigir la comunicación cuando se produzcan incidentes de este tipo.

4.5 De la distribución de claves al Internet cuántico

La distribución cuántica de claves es, por construcción, una tecnología que permite enviar secuencias de bits aleatorias punto a punto. Esta comunicación es incondicionalmente segura desde el punto de vista de la teoría de la información, pero no siempre lo es en la práctica por los problemas concretos derivados de su implementación. Además, QKD tiene un alcance limitado, pues los fotones que llevan la información se atenúan en su recorrido por el canal cuántico, lo que impide mantener la comunicación cuántica a largas distancias.

Para expandir las capacidades de QKD, comunicando más de dos usuarios y superando las limitadas distancias a las que pueden establecerse los enlaces cuánticos, es necesario desplegar una infraestructura que integre varios sistemas QKD conectados de forma segura, en lo que se conoce como **infraestructura de comunicaciones cuántica** (QCI, *Quantum Communications Infrastructure*). Este tipo de infraestructura debe incorporar nodos intermedios (repetidores) que permitan no solo evitar el problema del alcance limitado de QKD, sino también mitigar su baja tasa de generación de claves, como se verá en el siguiente apartado [158] [159].

Idealmente, los nodos de QCI deberían ser **repetidores cuánticos**, que fueran capaces de extender la señal cuántica sin necesidad de copiarla, manteniendo las propiedades cuánticas de los fotones transmitidos y, por consiguiente, la seguridad teórica en el canal. El desarrollo de estos repetidores es complejo, pues requiere de mecanismos para establecer entrelazamiento cuántico estable entre fotones y de memorias cuánticas confiables, tecnologías ambas que se aún se encuentran en fase de desarrollo experimental [160].

Como alternativa, las implementaciones actuales de QCI usan **repetidores clásicos**, que recuperan los bits de la señal de entrada y los retransmiten en la señal de salida, por lo que interrumpen la transmisión cuánticamente segura [116] [124]. Los usuarios de infraestructuras con repetidores clásicos deben confiar completamente en su seguridad, ya que tienen acceso a las claves transmitidas y además pueden fácilmente actuar como hombre en el medio. Por ello, los expertos consideran el uso de este tipo de repetidores como una solución temporal para seguir avanzando hacia QCI mientras se desarrollan los repetidores cuánticos.

En la actualidad hay numerosos proyectos de **QCI terrestre** en marcha por todo el mundo, que utilizan fibra óptica como medio de transmisión. Un ejemplo representativo es **MadQCI**, uno de los proyectos de este tipo de mayor envergadura en Europa [161]. MadQCI tiene como objetivo conectar el área metropolitana de Madrid con una infraestructura de comunicaciones cuánticas y, a más largo plazo, integrarse en la futura red de comunicaciones cuánticas europea desarrollada dentro del marco del programa EuroQCI [162]. En MadQCI participan actores tanto académicos como de telecomunicaciones, con la Universidad Politécnica de Madrid liderando la investigación, y Telefónica y RedIMadrid proporcionando la infraestructura de red necesaria [163].

Durante un periodo de prueba de tres años, en MadQCI se desplegaron 45 enlaces cuánticos directos integrando equipos QKD de diferentes fabricantes (ID Quantique, Toshiba Research Europe, Huawei, etc.) en una red heterogénea con un radio aproximado de 30 km en el área metropolitana de Madrid. La arquitectura de red es flexible, al estar controlada por SDN (*Software Defined Network*), lo que facilita la integración y gestión dinámica de diferentes tecnologías QKD en infraestructuras de red convencionales. Además de enlaces de fibra dedicados (DV-QKD), MadQCI permite la coexistencia de señales cuánticas y clásicas en la infraestructura de fibra madrileña (CV-QKD) demostrando la viabilidad de integrar QKD en redes comerciales de telecomunicaciones [161] [163].

Las QCI terrestres, que utilizan fibras ópticas y repetidores clásicos, están limitadas en cuanto a las distancias que pueden llegar a alcanzar por la alta atenuación en las fibras. Para lograr áreas de cobertura más extensas es fundamental recurrir a **QCI satelitales**, con satélites que actúen como nodos intermedios y conecten mediante enlaces cuánticos de espacio libre estaciones terrestres que pueden estar muy separadas entre sí y que, en muchos casos, sería imposible conectar por tierra debido a condicionantes geográficos [116] [158] [159]. La Figura 4-3 representa un ideal sistema de comunicaciones QKD con cobertura global, en el que se enlazan QCI terrestres distantes entre sí vía satélite para conseguir una infraestructura con gran área de cobertura.

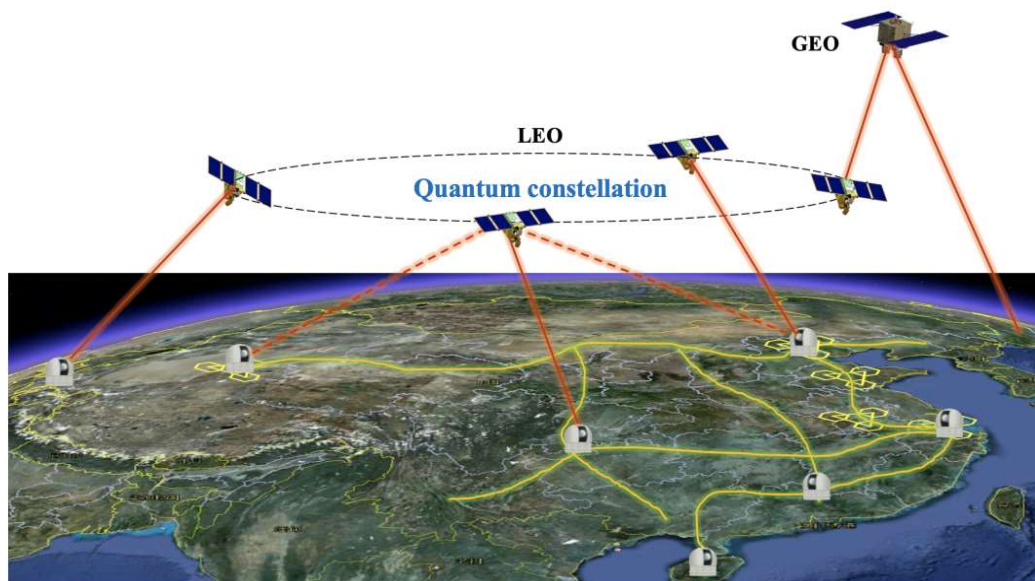


Figura 4-3 Comunicaciones a escala global combinando QKD terrestre y satelital [144].

El **QKD satelital**, sin embargo, se encuentra en pleno desarrollo y presenta importantes desafíos tecnológicos. Por un lado, las transmisiones a través de enlaces ópticos en el espacio son sensibles a las variaciones atmosféricas y las condiciones climáticas, que pueden distorsionar la señal cuántica e incluso llegar a inhabilitarla. Aunque más allá de atmósfera no hay prácticamente absorción, se produce también pérdida de señal por la difracción del haz de luz, aproximadamente proporcional al cuadrado de la distancia que recorre dicho haz. Por otro, los satélites requieren sistemas avanzados de seguimiento y de la alineación precisa de la instrumentación óptica de los equipos para garantizar que los haces de luz que transportan la señal cuántica estén perfectamente dirigidos entre los satélites y las estaciones terrestres que conectan [116] [144] [159].

Actualmente China lidera la investigación y desarrollo de QKD satélite a nivel mundial. En 2016, la Academia de las Ciencias de China lanzó desde Jiuquan el primer satélite dedicado a experimentación con QKD, conocido como **Micius** o Mozi, y logró ponerlo en operación en una órbita baja (**LEO**, *Low Earth Orbit*) de altitud aproximada 500 km [144] [164] [165]. En 2022, China lanzó un segundo satélite para QKD de mucho menor tamaño, llamado Jinan-1, aunque los resultados que ha publicado a día de hoy corresponden a experimentos llevados a cabo con Micius [166] [167].

Gracias a Micius se ha podido demostrar la viabilidad de establecer enlaces DV-QKD de espacio libre con satélites LEO en diferentes experimentos [144] [164], siendo el de mayor alcance la transmisión en 2024 de dos claves aleatorias entre las estaciones china de Nanshan y la rusa de Zvenigorod, que se encuentran separadas por unos 3.800 km entre sí [167]. Estas pruebas se realizaron durante la noche para evitar la interferencia de la luz solar y, además, las claves fueron transmitidas desde el satélite hacia las estaciones terrestres porque el equipamiento óptico de estas últimas es más avanzado. Otro experimento exitoso llevado a cabo con Micius consistió en distribuir un par de fotones entrelazados entre las estaciones terrestres de Delingha y Lijiang, a una distancia de unos 1.200 km, lo que confirmó que el entrelazamiento puede mantenerse estable incluso en esta escala [144].

Aunque en la actualidad los satélites chinos Micius y Jinan-1 son los únicos en órbita dedicados a QKD, a partir de 2025 está previsto el lanzamiento de más satélites LEO, como por ejemplo QUBE-II, Eagle-1 o QEYSSat. Por otra parte, dado que los satélites LEO solo son visibles en una posición determinada durante una ventana temporal específica, se pretende utilizar satélites en órbitas más altas.

Ya ha comenzado el desarrollo de satélites experimentales para órbita geostacionaria (**GEO**, *Geostationary Earth Orbit*), que al ubicarse en una posición fija respecto a La Tierra permitirían establecer enlaces cuánticos permanentes con las estaciones terrestres en su área de cobertura [166]. Destaca en este ámbito el proyecto europeo Caramuel [168], que se enmarca en el programa EuroQCI. El objetivo no es que los satélites GEO sustituyan a los LEO, sino que se complementen, creando una red multi-orbital que permita implementar redes de comunicaciones seguras intercontinentales.

La interconexión de QCI terrestres y satélites, junto con el desarrollo aún pendiente de nuevas tecnologías como los repetidores cuánticos y las memorias cuánticas, podrían idealmente derivar en el despliegue de una infraestructura global de comunicaciones en las que la seguridad estuviera garantizada por las propiedades de la física cuántica y resistir frente a cualquier adversario, con independencia de su capacidad computacional. Este potencial **Internet cuántico** no solo permitiría comunicaciones seguras a escala global, sino que además abriría la puerta a la integración de tecnologías cuánticas y permitiría el desarrollo de aplicaciones revolucionarias como la computación cuántica distribuida o las redes de sensores cuánticos de alta precisión [116] [117].

4.6 Redes de distribución cuántica de claves

Debido a las limitaciones de la tecnología QKD en la actualidad, la solución para aumentar la cobertura de soluciones QKD pasa por concatenar nodos capaces de establecer enlaces QKD e ir saltando entre ellos. Como se han de usar múltiples nodos, y generalmente dar servicio a múltiples usuarios, es preciso desplegar una **infraestructura de red** en la que estos nodos no solo sean capaces de establecer enlaces QKD, sino que además provean claves a las aplicaciones que lo demanden. Además, como en cualquier red clásica, es fundamental que los nodos puedan ser gestionados de forma segura y que la infraestructura sea mantenible y escalable [169] [170] [171].

El mecanismo habitual para transmitir una clave usando **nodos intermedios** es *hop-by-hop*, tal y como se representa en la Figura 4-4. El nodo emisor A genera una clave aleatoria *ran*, acuerda una clave K_{AB} por el enlace cuántico con el primer nodo intermedio B y le envía por un canal clásico el cifrado de *ran* con OTP usando como clave K_{AB} (es decir, $ran \oplus K_{AB}$). De la misma forma proceden los nodos B y C hasta que, finalmente, el nodo receptor D recupera *ran* descifrando con K_{CD} . Como puede apreciarse, es fundamental para la seguridad del esquema *hop-by-hop* que los nodos intermedios por los que transcurre la comunicación sean confiables, pues todos ellos conocen el secreto compartido [169] [170].

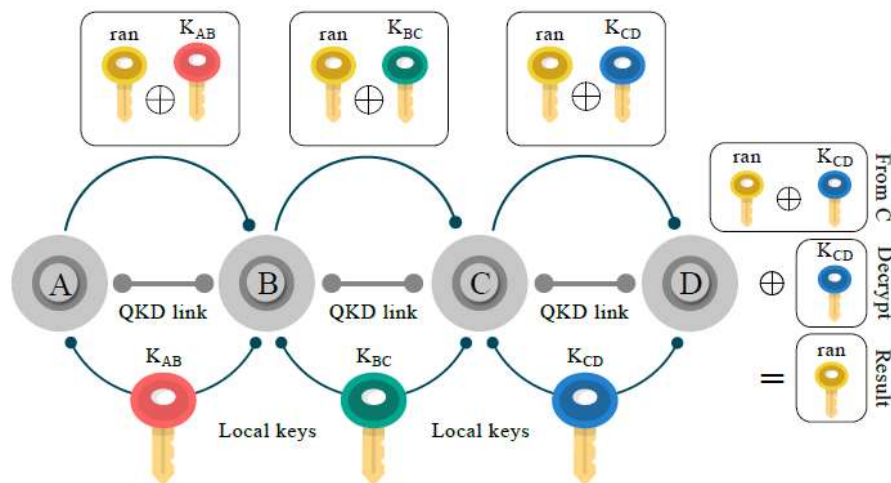


Figura 4-4 Distribución hop-by-hop de una clave empleando dos nodos intermedios [170].

Para implementar en la práctica una red QKD, los nodos de la red no pueden ser simplemente los equipos capaces de hacer la transmisión de bits aleatorios por el canal cuántico y concretar la clave por el canal auxiliar clásico. De hecho, se establecen **varias capas lógicas** en los nodos: la capa cuántica (con uno o varios equipos QKD), la capa de gestión de claves, la capa de control y la capa de servicio (donde se ubican las aplicaciones demandantes de claves). Por encima de estas capas en los nodos se establece, además, la funcionalidad de **gestión de la red de nodos** para optimizar la ruta de transmisión de claves en función de la disponibilidad de recursos y la demanda de las aplicaciones [170]. Habitualmente se emplea SDN (*Software Defined Network*) para la gestión de la red por su flexibilidad y eficiencia, pero su uso no es obligado.

En la Figura 4-5 a continuación se representa esquemáticamente esta arquitectura de red.

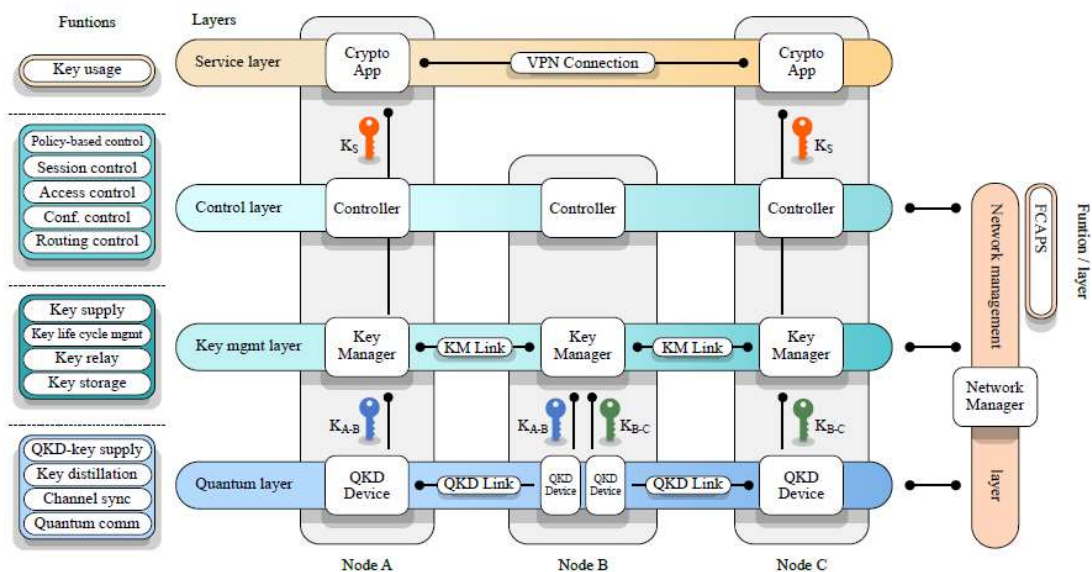


Figura 4-5 Arquitectura en capas de una red QKD [170].

Un componente fundamental de esta arquitectura es el **gestor de claves** (KM, Key Manager), que controla la generación de claves, su distribución y su consumo. El KMS genera claves de forma continuada interactuando con el equipamiento QKD del nodo, las almacena de forma segura y comparte qué claves ha generado con los KM de los demás nodos de la red por los que transcurre la comunicación. Además, el KM se encarga de gestionar el ciclo de vida de las claves asegurando, por ejemplo, que solo se sirven a la capa de servicio claves ya distribuidas a los demás nodos y que cada clave se elimina de forma segura después de su uso [169].

El proceso de **generación continuada** y almacenamiento de claves que orquesta el KM es fundamental para que las redes QKD sean viables, pues permite que las aplicaciones que demandan claves puedan disponer de ellas inmediatamente en lugar de que tener que esperar a que se complete su generación, mitigando así la limitación que supone la pobre tasa de generación de claves en QKD. Este tiempo de espera puede llegar a ser muy alto, dado que el proceso de distribución *hop-by-hop* a través de la red es lento al necesitar de varios intercambios QKD, cada uno con tasa de generación baja. De esta forma es posible establecer enlaces cifrados estables con claves derivadas cuánticamente, como en la prueba realizada recientemente [171], en la que se logró operar establecer durante 45 días túneles IPSEC entre dos ubicaciones conectadas por fibra a 46 km de distancia, llegando a alcanzar los 100 Gbps.

Respecto a los interfaces de las diferentes componentes de la arquitectura de red QKD y los protocolos de comunicación entre ellas, se han desarrollado diferentes **estándares**. La organización que cuenta con un mayor número de estándares es ETSI, que ha publicado normas importantes para el despliegue de redes QKD, a destacar GS-QKD-014 [172] (API REST para que las aplicaciones obtengan claves del KM), GS-QKD-004 [173] (introducción de parámetros de QoS en las sesiones) y GS-QKD-015 [174] (interfaces de control de la red de nodos usando SDN). Sin embargo, aún faltan estándares para otros elementos relevantes, como es la comunicación entre los KM de los nodos de la red, un aspecto fundamental para asegurar que las claves se sincronizan correctamente [169] [170].

Además, no existe a día de hoy consenso en cuanto a qué estándares utilizar al implementar redes QKD, ni entre los fabricantes de equipos ni en los proyectos desarrollados de QCI, produciéndose incluso variaciones de la arquitectura con respecto a la planteada en esta sección. Este problema, junto con la indefinición de algunos interfaces y protocolos, limita la **escalabilidad** de los proyectos QCI, que habitualmente integran tecnologías de distintos proveedores, y afecta a su **interoperabilidad** [169]. Si bien esto ya supone un condicionante serio para desplegar redes QKD metropolitanas, se tornará aún más crítico al intentar integrar estas redes y extender la cobertura del uso de QKD en el camino hacia el ideal del Internet cuántico.

4.7 Controversia sobre la idoneidad de QKD para resistencia cuántica

A lo largo de esta sección se han presentado los fundamentos de la distribución cuántica de claves, así como su utilidad para compartir un secreto entre dos partes por un canal cuántico con la garantía de que no pueda ser interceptado inadvertidamente por un actor malicioso. Además, se han descrito las limitaciones prácticas que tienen las soluciones QKD en la actualidad, los retos a los que se enfrentan y los problemas de seguridad que presentan más allá de la seguridad teórica incondicional que ofrece la transmisión cuántica en sí. Asimismo, se ha señalado que, debido a la falta de repetidores cuánticos, la extensión del alcance de QKD depende del despliegue de redes con múltiples nodos intermediarios confiables en la comunicación.

En los últimos años, varios **gobiernos han desaconsejado el uso de QKD** para garantizar la seguridad frente a un CRQC, apostando de forma decidida por la criptografía post-cuántica. En estos términos se han manifestado instituciones de seguridad como la NSA (Estados Unidos) [175], el BSI (Alemania) [176], el NCSC (Reino Unido) [177] y el ANSSI (Francia) [178], entre otros. La NSA va más allá de una simple recomendación y afirma que no tiene previsto certificar ningún sistema QKD para proteger las comunicaciones en sistemas de seguridad nacional.

El primer argumento que comparten estas agencias es que la seguridad real que proporciona un sistema QKD no es la seguridad teórica incondicional que garantiza la física cuántica, como se declara a menudo en este ámbito. La razón es que los sistemas QKD son muy complejos de implementar, por lo que **sus instancias concretas se desvían del ideal teórico** y suelen ser susceptibles a ataques prácticos relacionados con las propiedades físicas de los dispositivos empleados en su implementación. Además, la exposición de los sistemas QKD a ataques de denegación de servicio es elevada, lo que puede plantear problemas serios de disponibilidad.

Estas agencias también coinciden en que QKD es una **solución parcial** a la amenaza cuántica, ya que, aunque permite transporte de claves y puede por tanto usarse para garantizar la confidencialidad, no proporciona un medio para garantizar la autenticidad del emisor. La seguridad de cualquier sistema QKD que no implemente una autenticación robusta entre los comunicantes en el canal auxiliar se vería comprometida por un ataque de hombre en el medio [145]. Por ello, los sistemas QKD requieren de un mecanismo de autenticación, ya sea mediante el uso de claves pre-compartidas o, de manera más general, a través de esquemas de firma digital basados en algoritmos de clave pública.

La **falta de madurez de la tecnología** es otro de los inconvenientes que ven estas agencias a la hora de garantizar la seguridad de los sistemas QKD. Consideran que queda aún camino por recorrer en lo que concierne a la seguridad de los dispositivos específicos que precisa QKD, así como en el establecimiento de estándares, pruebas de seguridad y criterios de evaluación. En cambio, la criptografía post-cuántica está más madura (ya hay estándares y se están integrando en protocolos) y cuenta además con la ventaja de que puede implementarse en hardware clásico, lo que facilita su despliegue en infraestructuras de comunicación tradicionales.

Finalmente, otro argumento en contra de la adopción de QKD que esgrimen estas agencias es que las redes QKD necesitan una **costosa infraestructura dedicada**, por lo que no parece razonable su universalización a medio plazo. Por un lado, estas redes precisan de equipamiento especial para establecer canales cuánticos que, al no estar implementado en software, no se integra fácilmente con los equipos de red clásicos y es poco flexible para actualizaciones o parches de seguridad. Por otro lado, las redes QKD necesitan nodos intermedios confiables que deben ser convenientemente protegidos, lo que también eleva considerablemente su coste. En cambio, la opción de la criptografía post-cuántica permite resistir a la amenaza cuántica utilizando la infraestructura de Internet actual.

Por todo ello, NSA, BSI, NCSC y ANSSI consideran que QKD no es adecuado para la mayoría de los casos prácticos y que su uso solo estará justificado en situaciones donde los requisitos de seguridad específicos lo requieran y se justifique su elevado coste. Además, opinan que dada la **urgencia** de comenzar a abordar la transición hacia un Internet con resistencia cuántica, la apuesta por la criptografía post-cuántica se perfila como una opción más viable a corto y medio plazo.

5 CRIPTOGRAFÍA POST-CUÁNTICA

En esta sección se introduce la criptografía post-cuántica (PQC, *Post-Quantum Cryptography*), que también es conocida como criptografía resistente a la computación cuántica. Se trata de una solución alternativa a las comunicaciones cuánticas para el desarrollo de criptosistemas que puedan garantizar los servicios de seguridad no solo respecto a los adversarios actuales, sino también frente a un hipotético atacante que disponga de un CRQC. Se aborda cómo esta disciplina se centra en el diseño de nuevos algoritmos de clave pública, dado que los actuales basan su seguridad computacional en problemas que, teóricamente, resultarán abordables para los ordenadores cuánticos del futuro.

Se describe como, para garantizar la seguridad de los nuevos algoritmos de clave pública, se han adoptado problemas matemáticos alternativos a los de factorización y logaritmo discreto que constituyen la base de los algoritmos actuales. También se explica cómo, además de los esquemas clásicos de cifrado y firma digital, la criptografía post-cuántica ha promovido el concepto de encapsulamiento de claves en detrimento del uso del acuerdo de claves clásico con DH o ECDH. La razón detrás de este cambio es que resulta sencillo garantizar la robustez de un KEM (*Key Encapsulation Mechanism*) a partir de condiciones de seguridad menos exigentes del cifrado de clave pública en el que se basa.

Desde que en 2016 el NIST inició un concurso para la evaluación de algoritmos post-cuánticos, se han desarrollado y sometido a escrutinio público decenas de algoritmos basados en construcciones matemáticas diversas, todas ellas consideradas a priori resistentes a la computación cuántica, que se describen de manera general. Aunque este concurso sigue en marcha, el NIST ya ha estandarizado los tres primeros algoritmos post-cuánticos: un encapsulamiento basado en retículos y dos firmas digitales, una también basada en retículos y la otra en árboles de funciones *hash*. Durante estos años, muchos de estos algoritmos han sido atacados, algunos incluso en las fases finales del concurso.

Se deduce que los algoritmos post-cuánticos son más complejos que los utilizados en criptografía clásica, lo que dificulta garantizar su seguridad tanto desde el punto de vista formal como en sus implementaciones. También se detalla que estos algoritmos suelen ser más costosos, tanto en longitud de claves, cifrados y firmas, como en rendimiento. Es por ello que, en algunos casos, se ha introducido estructura adicional al problema matemático base de algún algoritmo para hacerlo más eficiente, lo que supone una reducción de su margen de seguridad y potencialmente una ventana de oportunidad para los adversarios.

Para concluir se explica que, aunque ya se han empezado a integrar algoritmos PQC en algunos protocolos criptográficos, no será inmediato que estos algoritmos reemplacen completamente a los de clave pública actuales en Internet. El mayor coste de los nuevos algoritmos y la necesidad de sustituir DH por KEM son las dos principales dificultades para esta integración. De hecho, se prevé que esta transición hacia la criptografía post-cuántica sea un proceso largo, complejo y costoso. Durante los próximos años, es razonable esperar que se apueste por la hibridación de algoritmos clásicos y post-cuánticos, con objeto de minimizar los riesgos de seguridad que supone el cambio de un conjunto de algoritmos maduros por otros más nuevos que aún están bajo el escrutinio de la comunidad científica.

5.1 Criptografía (de clave pública) post-cuántica

La **criptografía post-cuántica**, conocida como **PQC** por sus siglas en inglés (*Post-Quantum Cryptography*), es una rama de la criptografía orientada al desarrollo de algoritmos que puedan ser utilizados en sistemas informáticos y de comunicaciones convencionales y sean capaces de resistir ataques de un adversario cuántico (un adversario con acceso a un CRQC) [118]. PQC a veces también se referencia en la literatura científica como criptografía con resistencia cuántica o cuánticamente resistente, términos que, aunque describen mejor la disciplina, tienen un uso mucho menos extendido.

Ante el avance de la computación cuántica y la amenaza que implica para la criptografía tradicional y la seguridad de los sistemas TIC, en los últimos años la comunidad criptográfica ha desarrollado **nuevos algoritmos** de este tipo. Aunque no hay una fecha exacta para el origen de PQC, el congreso PQCrypto de 2006 es considerado por muchos expertos como punto de partida para el desarrollo de esta disciplina [179]. Un hito fundamental en su evolución fue el concurso de estandarización que lanzó el instituto NIST en 2016 [65], que aceleró notablemente la investigación en PQC, y que ha logrado recientemente la publicación de los tres primeros estándares de PQC [180].

Aunque el término PQC hace referencia a criptografía en general, en realidad se están desarrollando algoritmos de **clave pública**, pues son las primitivas clásicas de este tipo las que se encuentran seriamente amenazadas por la eficiencia de los algoritmos de factorización cuántica como el de Shor y sus versiones optimizadas. Por el contrario, los algoritmos de cifrado simétrico se consideran suficientemente seguros frente a la computación cuántica siempre que utilicen una longitud de clave suficientemente larga (ídem para las funciones *hash* y las primitivas construidas a partir de ellas), dado que el algoritmo de Grover reduce su nivel de seguridad a la mitad.

Los algoritmos simétricos con claves de 256 bits utilizados a día de hoy ofrecen un nivel de seguridad de 128 bits frente a un CRQC, lo que se considera suficiente en la actualidad. Además, ya existen algunos algoritmos con claves de hasta 512 bits, como por ejemplo Threefish [181], y se han desarrollado diversas técnicas para crear algoritmos simétricos con claves más largas, como las cascadas de algoritmos de cifrado en bloque [182]. Sin embargo, a pesar de la creencia extendida fuera del ámbito de la criptografía de que es posible duplicar la clave de cualquier algoritmo simétrico para incrementar la seguridad, estas técnicas de extensión de clave no logran alcanzar este ideal.

La seguridad de los algoritmos de clave pública actuales se basa en la complejidad computacional de dos problemas matemáticos, la factorización entera y el cálculo del logaritmo discreto en un grupo finito, para instancias suficientemente grandes. Dado que estos problemas son a priori resolubles en un CRQC en tiempo polinomial, los nuevos algoritmos post-cuánticos basan su seguridad en **problemas matemáticos alternativos** a la factorización y el logaritmo discreto. Estos problemas alternativos deben ser intratables tanto para ordenadores cuánticos como clásicos. Las matemáticas base que se han utilizado hasta ahora para fundamentar el desarrollo de nuevos algoritmos de clave pública cuánticamente resistentes son principalmente: retículos o *lattices*, códigos de corrección de errores, funciones *hash*, polinomios multivariantes en campos finitos e isogenias de curvas elípticas [118].

Se están desarrollando tres tipos de algoritmo en PQC: **PKE** (*Public Key Encryption*), **KEM** (*Key Encapsulation Mechanism*) y **DS** (*Digital Signature*). Mientras que los algoritmos PKE y DS en PQC son equivalentes al cifrado con clave pública y la firma digital clásicos, los KEM limitan la función de cifrado a un espacio de claves aleatorias en lugar de abarcar el espacio de mensajes como ocurre en PQC-PKE. El concepto de KEM surge de manera natural debido al uso híbrido de criptografía simétrica y asimétrica en los protocolos criptográficos para el establecimiento de claves de sesión [183].

La diferencia entre PKE y KEM se muestra en la Figura 5-1. Un PKE está compuesto por las funciones Gen/Encrypt/Decrypt y un KEM por Gen/Encap/Decap. La primera función es similar en ambos casos: $(sk, pk) = \text{Gen}(s)$ genera par de claves privada sk y pública pk para el algoritmo asimétrico en uso de acuerdo al nivel de seguridad s . En un PKE, la función $c = \text{Encrypt}(pk, m)$ cifra un mensaje m con la clave pk y la función $m = \text{Decrypt}(sk; c)$ descifra el cifrado c con la clave sk para recuperar el mensaje m original. En un KEM, la función $(k, c) = \text{Encap}(pk)$ genera una clave aleatoria k y la cifra (encapsula) usando la clave pk , mientras que $k = \text{Decap}(sk, c)$ descifra y recupera la clave k . Tanto Decrypt como Decap pueden devolver $\perp$ en caso de error.

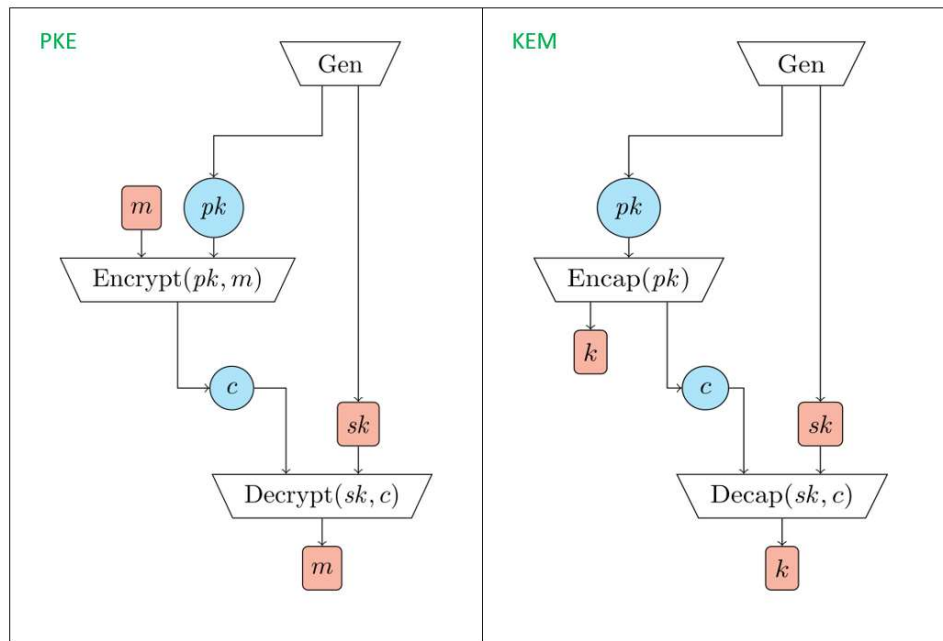


Figura 5-1 Diagramas de los esquemas PKE y KEM [184] [185].

Un KEM es, por construcción, un esquema de transporte de claves. En PQC se ha apostado por esta primitiva criptográfica y **se ha obviado el uso de DH**, que en criptografía clásica constituye el mecanismo principal para acuerdo de claves en protocolos criptográficos. El propio NIST justifica que el uso de DH en protocolos puede ser reemplazado por KEM, lo que recomienda al tratarse de una primitiva con una definición de seguridad más clara y aceptada que DH y que resulta eficiente en la generación de claves de sesión [186]. Por tanto, la adaptación post-cuántica de un buen número de AKE utilizados en los protocolos criptográficos actuales pasa por reemplazar DH por KEM, o combinar ambas primitivas, lo que supone un importante desafío.

5.2 Proceso de estandarización del NIST

Para entender el estado del arte de PQC es relevante revisar el proceso de **estandarización** llevado a cabo por el instituto estadounidense NIST, que empezó en 2016 y que ha llevado a la publicación en agosto de 2024 de los tres primeros estándares FIPS en esta disciplina [65] [180] [188]. Durante estos años los algoritmos han sido evaluados en función de su seguridad frente a diferentes tipos de ataques, de su rendimiento en implementaciones y de su flexibilidad [189].

Este proceso ha consistido en varias rondas de evaluación [190]. La **primera ronda** comenzó en diciembre de 2016, cuando el NIST invitó a la comunidad criptográfica a presentar algoritmos PQC. Esta ronda finalizó en julio de 2019, y durante este periodo se presentaron un total de 82 propuestas. Tras su evaluación, se seleccionaron 17 algoritmos de KEM y 9 de DS para pasar a una **segunda ronda** en la que fueron analizados más exhaustivamente. Esta fase concluyó en julio de 2020 con la selección de 7 finalistas (4 KEM y 3 DS) y 8 candidatos alternativos (5 KEM y 3 DS).

La **tercera ronda** de evaluación finalizó en julio de 2022 con la propuesta de estandarización de 1 algoritmo de KEM y 3 de DS, además del anuncio de una **cuarta ronda** para seguir evaluando otros 4 KEM, ronda que sigue en curso a día de hoy. En agosto de 2024 el NIST aprobó un estándar para KEM, el **FIPS-203** (CRYSTALS-KYBER) [191], y dos para DS, el **FIPS 204** (CRYSTALS-DILITHIUM) [192] y el **FIPS 205** (SPHINCS+) [193], anunciando además que sigue desarrollando el estándar correspondiente a la firma FALCON [180].

La Tabla 5-1 recopila los algoritmos que llegaron a las fases finales del concurso y el resultado de su evaluación hasta el momento:

Algoritmo	Tipo	Resultado ronda 2	Resultado ronda 3
CRYSTALS-KYBER	KEM	Pasa a ronda 3	Se estandariza
Classic-McEliece	KEM	Pasa a ronda 3	Pasa a ronda 4
NTRU	KEM	Pasa a ronda 3	
SABER	KEM	Pasa a ronda 3	
BIKE	KEM	Alternativo	Pasa a ronda 4
HQC	KEM	Alternativo	Pasa a ronda 4
SIKE	KEM	Alternativo	Pasa a ronda 4
FrodoKEM	KEM	Alternativo	
NTRU Prime	KEM	Alternativo	
CRYSTALS-DILITHIUM	DS	Pasa a ronda 3	Se estandariza
FALCON	DS	Pasa a ronda 3	Se estandariza
Rainbow	DS	Pasa a ronda 3	
SPHINCS+	DS	Alternativo	Se estandariza
GeMSS	DS	Alternativo	
Picnic	DS	Alternativo	

Tabla 5-1. Algoritmos PQC en las fases finales del concurso del NIST [190].

Como se puede observar, el NIST ha optado por desarrollar **varios estándares de KEM y DS** [180] [190]. Por una parte, se busca ofrecer a la comunidad algoritmos basados en diferentes fundamentos matemáticos para tener un “plan B” en caso de que, en el futuro, se encontraran vulnerabilidades críticas en alguna familia de algoritmos. En la actualidad, el KEM definido en FIPS 203 se basa en retículos y los candidatos a KEM que continúan en concurso emplean ya sea códigos (3) o isogenias (1), mientras que los DS estandarizados en FIPS 204 y FIPS 205 utilizan, respectivamente, retículos y funciones *hash*.

Por otra parte, las prestaciones de los algoritmos PQC varían considerablemente (la longitud de clave, la velocidad de ejecución de las funciones, la longitud de encapsulados y firmas, etc.), por lo que conviene contar con diferentes opciones que permitan seleccionar el algoritmo más adecuado según el caso de uso para garantizar resistencia cuántica. Por ejemplo, aunque CRYSTALS-DILITHIUM (FIPS 204) y FALCON están ambos basados en retículos, FALCON genera firmas más cortas, lo que puede ser preferible en aplicaciones donde el tamaño de la firma sea un factor limitante.

Respecto a los **criterios de evaluación** definidos por NIST [189], se han tenido en cuenta aspectos relativos a la seguridad de las primitivas criptográficas, a su rendimiento y su flexibilidad. En lo relativo al rendimiento, se han considerado factores como la eficiencia computacional de las operaciones, la longitud de las claves públicas, el tiempo de generación de claves y el tamaño de los datos que se generan (cifrados, encapsulados o firmas). En lo que respecta a la flexibilidad, se ha valorado positivamente la simplicidad tanto del diseño como en las implementaciones en diferentes plataformas, ya sean software o hardware, así como la adaptabilidad a los diferentes protocolos criptográficos.

En cuanto a la seguridad de los algoritmos PQC, NIST ha exigido el cumplimiento de las nociones de seguridad más estrictas para las primitivas KEM y DS. Los algoritmos **KEM deben ser IND-CCA2**: un adversario no puede distinguir entre dos claves encapsuladas, aunque tenga acceso al encapsulado de otras claves y pueda enviarlas a un oráculo de desencapsulado (al que, obviamente, no puede consultar el encapsulado específico que está atacando). Además, los algoritmos **DS deben ser EUF-CMA**: un adversario no puede conseguir la firma de un mensaje que no haya sido legítimamente firmado, aunque tenga acceso a un oráculo con el que pueda firmar cualquier mensaje distinto del que quiere falsificar.

Existen técnicas criptográficas que permiten convertir en un KEM con seguridad IND-CCA2 cualquier algoritmo PKE con una seguridad básica IND-CPA (el adversario no accede a un oráculo de descifrado, como ocurre en IND-CCA2, pero sí a un oráculo de cifrado con el que puede cifrar mensajes a su elección). La técnica más extendida es la **transformada de Fujisaki-Okamoto** [187], en la cual se combina el uso de las funciones del algoritmo PKE con funciones *hash*, que ha sido utilizada por la mayoría de los candidatos a KEM basados en retículos que se han presentado al concurso para alcanzar la seguridad IND-CCA2 requerida.

Para evaluar la seguridad de los algoritmos PQC, NIST ha definido **5 niveles de seguridad** en función de los recursos computacionales, ya sean clásicos o cuánticos, necesarios para vulnerar la seguridad de ciertas primitivas criptográficas simétricas (ver Tabla 5-2). Los algoritmos post-cuánticos de KEM y DS desarrollados se parametrizan según estos niveles de seguridad. Aunque se estima que los niveles 1, 2 y 3 proporcionarán un margen de seguridad suficiente para el futuro previsible, se introducen los niveles 4 y 5 para conseguir una protección mayor frente potenciales avances en criptoanálisis o en tecnologías computacionales.

Nivel seguridad	Complejidad del ataque
1	Recursos computacionales comparables o mayores a los requeridos para la búsqueda de claves en un cifrador de bloques con clave de 128 bits.
2	Recursos computacionales comparables o mayores a los requeridos para la búsqueda de colisiones en una función <i>hash</i> de 256 bits.
3	Recursos computacionales comparables o mayores a los requeridos para la búsqueda de claves en un cifrador de bloques con clave de 192 bits.
4	Recursos computacionales comparables o mayores a los requeridos para la búsqueda de colisiones en una función <i>hash</i> de 384 bits.
5	Recursos computacionales comparables o mayores a los requeridos para la búsqueda de claves en un cifrador de bloques con clave de 256 bits.

Tabla 5-2. Niveles de seguridad para los algoritmos PQC definidos por NIST [189].

5.3 Fundamentos matemáticos en criptografía post-cuántica

Los algoritmos post-cuánticos basan su seguridad en la **complejidad computacional** de problemas matemáticos distintos a la factorización entera y el cálculo de logaritmos discretos, que son utilizados por los algoritmos de clave pública clásicos y resultan vulnerables ante un adversario cuántico. Hasta la fecha, se han desarrollado algoritmos a partir de retículos, códigos de corrección de errores, funciones *hash*, polinomios multivariantes en campos finitos, isogenias de curvas elípticas e incluso pruebas de conocimiento cero. La estructura de estos problemas sugiere que los algoritmos construidos sobre ellos pueden ser resistentes tanto a la computación clásica como a la cuántica [118] [188] [194].

En la Figura 5-2 se presentan los algoritmos PQC que llegaron a las fases finales del concurso NIST, enumerados en la Tabla 5-1, agrupados según el tipo de problema matemático en el que se fundamenta su seguridad. Se puede observar que la familia más representada es la criptografía basada en retículos, de la cual provienen dos de los tres algoritmos estandarizados hasta la fecha [180]. A lo largo de esta sección se describen de forma superficial los fundamentos de seguridad de cada una de estas familias junto con sus algoritmos representativos.

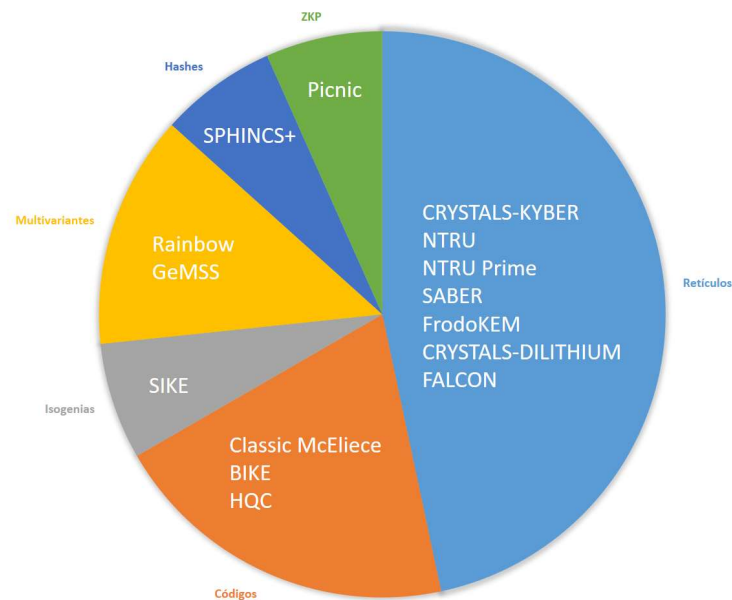


Figura 5-2 Familias de algoritmos PQC según su fundamento matemático.

La técnica más extendida para la construcción de algoritmos PQC es utilizar problemas en **retículos** [118] [197]. Un retículo es un conjunto discreto de puntos espaciados regularmente, que se obtienen como combinación lineal entera de los vectores de una base del espacio vectorial que se utilice (si la base la componen N vectores independientes, cada punto del retículo será un vector de N componentes). Esta sencilla estructura matemática comprende varios problemas con complejidad exponencial en un ordenador clásico, que se estima tendrán también esta complejidad en un CRQC. Los problemas clásicos de retículos que se consideran seguros son el SVP (*Short Vector Problem*), que consiste en encontrar el vector no nulo en el retículo con la menor longitud en la rejilla, y el CVP (*Closest Vector Problem*), en el que se busca el vector del retículo más cercano a un punto dado, aunque hay muchos otros como el SIVP (*Shortest Independent Vectors Problem*) o el GapSVP (*Gap Shortest Vector Problem*).

Los dos primeros algoritmos criptográficos basados en retículos se definieron a finales de la década de 1990: **GGH** (llamado así por las iniciales de sus creadores, Goldreich, Goldwasser y Halevi) [195] y **NTRU** (*Nth-degree Truncated Polynomial Ring Units*) [196], debido a Hoffstein, Pipher y Silverman. En 2005, Regev introdujo el problema de aprendizaje con errores (**LWE**, *Learning With Errors*) [198] que sirve de base para la mayor parte de los algoritmos actuales basados en retículos por ser mucho más práctico que GGH y NTRU. Más concretamente, los algoritmos PQC se construyen sobre sus variantes **MLWE** (Modular LWE) [199] y **RLWE** (Ring LWE) [200] [201], que utilizan anillos de polinomios en lugar de números enteros para dotar de estructura a los retículos y permitir implementaciones más eficientes que el LWE original.

Cinco KEM basados en retículos llegaron a las fases finales del concurso NIST: **CRYSTALS-KYBER** [202], **SABER** [203], **FrodoKEM** [204], **NTRU** y **NTRU-Prime** [205], resultando CRYSTALS-KYBER el primer ganador y siendo estandarizado como **ML-KEM** en el FIPS-203 [191]. Mientras que CRYSTALS-KYBER y SABER se fundamentan en MLWE, FrodoKEM está basado en el problema LWE original, y es, por tanto, más robusto desde el punto de vista teórico pero menos eficiente. Por otra parte, NTRU-Prime es una variante del NTRU original en la que el anillo de polinomios no se reduce con $x^N - 1$, sino con un polinomio irreducible que evita algunas simetrías en la estructura del esquema clásico, lo que lo hace menos eficiente, pero a priori más resistente frente a ataques algebraicos.

Los retículos también se han utilizado para definir DS, siendo dos de los ganadores NIST los algoritmos **CRYSTALS-DILITHIUM** [206] y **FALCON** [207]. El primero de ellos, que ya se ha estandarizado como **ML-DSA** en el FIPS 204 [192], basa su seguridad en M-LWE (al igual que ML-KEM), mientras que FALCON se fundamenta en el problema clásico SVP en lugar de en LWE y sus variantes. Como se verá en la sección 5.5, FALCON permite utilizar claves y firmas más pequeñas, pero su función de generación de claves es mucho más ineficiente que la de ML-DSA.

La reducción de la seguridad en pro de la eficiencia en los esquemas basados en retículos estructurados es una cuestión controvertida. Hasta ahora, el NIST ha priorizado la eficiencia al favorecer el uso de CRYSTALS-KYBER (M-LWE) frente a FrodoKEM (LWE), con el objetivo de favorecer su adopción como alternativa a los algoritmos de clave pública clásicos amenazados cuánticamente. Sin embargo, esta apuesta por la eficiencia puede tener un impacto negativo en la seguridad de los algoritmos, pues abre la posibilidad de que un adversario pueda aprovechar la estructura de los retículos para desarrollar ataques algebraicos. De hecho, otros organismos como el BSI alemán han sido más conservadores y recomiendan FrodoKEM, aun siendo más ineficiente [208].

Por otra parte, los **códigos correctores de errores** también permiten diseñar esquemas criptográficos post-cuánticos, cuya seguridad se sustenta en la complejidad del problema de decodificar un mensaje codificado con un código aleatorio o no estructurado [118] [188] [194]. El primer criptosistema de este tipo fue diseñado en 1978 por McEliece [209], un algoritmo de clave pública que utiliza códigos binarios de Goppa, que son a priori indistinguibles de códigos lineales aleatorios, cuya seguridad estructural no ha podido ser vulnerada desde su creación. En 1986, Niederreiter [210] desarrolló una variante de McEliece con el mismo nivel de seguridad pero que permitía reducir la longitud de las claves, lo cual es sin duda el mayor inconveniente de este tipo de algoritmos.

Un grupo de investigadores liderado por Bernstein presentó al concurso del NIST una ligera modificación de la versión dual de Niederreiter del algoritmo de McEliece que lo transforma en un KEM, a la que denominaron **Classic-McEliece** [211]. Este algoritmo continúa siendo evaluado en la ronda 4, junto con otros dos algoritmos basados en códigos, **BIKE** (*Bit Flipping Key Encapsulation*) [212] y **HQC** (*Hamming Quasi-Cyclic*) [213]. Tanto BIKE como HQC emplean códigos estructurados, lo que les permite reducir significativamente el tamaño de la clave pública, pero su seguridad no está tan contrastada como la de Classic-McEliece. El NIST tiene la intención de seleccionar alguno de estos tres candidatos tras finalizar la ronda 4 para su estandarización [190].

Tal y como ocurre en criptografía reticular, la reducción del margen de seguridad que supone el uso de códigos estructurados respecto a los códigos de Goppa para mejorar la usabilidad de los KEM basados en códigos genera posiciones encontradas en la comunidad criptográfica. Los códigos cuasi-cíclicos, cuasi-diádicos o cuasi-monoidicos permiten una compresión de la clave pública de los algoritmos que los utilizan, haciendo más usables, pero esta compresión implica una reducción de la seguridad generalmente proporcional al factor de compresión que se consigue para la clave pública. De hecho, ha sido posible atacar algunos códigos estructurados de forma eficiente [214] [215].

Otra familia clásica de algoritmos DS post-cuánticos son los basados en **funciones hash**, cuya seguridad se fundamenta en propiedades bien conocidas de estas funciones, tales como la resistencia a pre-imágenes y la resistencia a colisiones. Este tipo de firma fue propuesto por Merkle en la década de 1970 [216], a quién se debe la estructura de árbol que implementan estos algoritmos en combinación con esquemas de firma de uso único. El uso de la estructura de árbol de Merkle permite que múltiples mensajes puedan ser firmados con una única clave de forma segura [188] [194].

Uno de los ganadores del concurso del NIST es precisamente **SPHINCS+**, un algoritmo de firma basado en funciones hash que se ha estandarizado con el nombre **SLH-DSA** (*StateLess Hash-based Digital Signature Algorithm*) en el FIPS 205 [193]. Como se verá en la sección 5.5, este algoritmo tiene un tamaño de firma y un coste computacional de generación de claves y firmas muy superior a otros algoritmos PQC, por lo que sus casos de uso son limitados. A pesar de ello, se considera un esquema muy seguro y el NIST ha apostado por él como una opción conservadora que podría ser utilizada en caso de que otros algoritmos de firma digital llegaran a ser comprometidos en el futuro.

La seguridad de la criptografía **multivariante** se fundamenta en la complejidad computacional que tiene la resolución de sistemas de ecuaciones polinómicas multivariantes sobre campos finitos, una construcción versátil que puede aplicarse para construir tanto esquemas de cifrado como de firma digital. En particular, su uso en algoritmos DS tiene la ventaja de que permite obtener firmas de longitud menor que otras alternativas de PQC [188].

Los algoritmos más conocidos de la familia multivariante son **Rainbow** [217] y **GeMSS** [218], que llegaron a la tercera ronda del concurso NIST como finalista y candidato alternativo, respectivamente. Sin embargo, en los últimos años se han revelado ataques para ambos algoritmos que explotan su estructura algebraica interna y permiten una reducción significativa de la seguridad conjeturada para los mismos [219] [220] [221] [222]. A pesar de que continúa la investigación en este ámbito, a día de hoy muchos expertos se muestran escépticos respecto a la idoneidad de este problema matemático para construir primitivas post-cuánticas.

En los algoritmos criptográficos de **isogenias** la seguridad se basa en la dificultad de encontrar una isogenia particular entre dos curvas elípticas dadas [188]. Una isogenia es un homomorfismo entre dos curvas elípticas que mapea los puntos de una curva a la otra y preserva la estructura de grupo. Es posible representar en grafos las conexiones entre curvas elípticas a través de isogenias, donde cada curva es un nodo y las aristas son las isogenias entre nodos. Cuando las curvas elípticas son supersingulares, estos grafos de isogenias son densos y presentan numerosas conexiones, lo que hace que el problema de encontrar una isogenia específica entre dos curvas sea computacionalmente complejo.

Hasta la ronda 4 del concurso de NIST llegó un único algoritmo basado en isogenias, un KEM llamado **SIKE** (*Supersingular Isogeny Key Encapsulation*) [223]. Este esquema fue atacado poco después y los autores lo retiraron del concurso [224] [225], por lo que no está prevista la estandarización de ningún algoritmo de este tipo por el momento. Ahora bien, la investigación en este campo continua, ya que el ataque no afecta a otros esquemas basados en isogenias en desarrollo, como el algoritmo de firma SQIsign o el de acuerdo de claves CSIDH [225].

Tras la ronda 2 del concurso NIST quedó como algoritmo alternativo de firma digital **Picnic** [226]. Más que un algoritmo, Picnic es un esquema basado en **pruebas de conocimiento cero** y en algoritmos simétricos de **cifrado en bloque**, que puede ser instanciado con diferentes primitivas de este tipo para construir algoritmos concretos, característica que le otorga una gran flexibilidad. A pesar de ser una alternativa novedosa y prometedora frente a los DS anteriores, Picnic no fue seleccionado como finalista debido a su falta de madurez y a problemas de eficiencia: genera firmas grandes y los tiempos de ejecución de las funciones de creación y verificación de firmas son lentos [194]. Además, el cifrado simétrico LowMC, que forma parte de la versión de Picnic presentada al concurso del NIST, ha sido recientemente criptoanalizado [227].

5.4 Seguridad de los algoritmos post-cuánticos

Los algoritmos post-cuánticos pretenden ser la piedra angular sobre la que se construya la seguridad de las comunicaciones en Internet frente a adversarios, tanto clásicos como cuánticos, en los próximos años. El avance de la computación cuántica y la posibilidad de que se pueda llegar a construir un CRQC en la próxima década han acelerado la investigación y el desarrollo de algoritmos PQC que sean capaces de proporcionar los servicios de seguridad que hoy día garantizan algoritmos de clave pública clásicos que serían vulnerables a los ataques cuánticos.

Gracias al gran esfuerzo de la comunidad científica especializada en criptografía en los últimos años, se han desarrollado algoritmos post-cuánticos de KEM y DS, algunos de los cuales incluso se han estandarizado y pueden ser ya implementados en productos y servicios. Estos nuevos esquemas criptográficos se construyen sobre modelos matemáticos como retículos, códigos, isogenias, etc., cuya dificultad computacional garantiza su seguridad frente a adversarios con acceso a un CRQC, como retículos, códigos, isogenias, etc. Se trata de **modelos más complejos** que los utilizados en criptografía clásica (factorización entera y logaritmo discreto) y que, por ello, tienden a ser más ineficientes que sus alternativas clásicas en términos de coste computacional y longitudes de claves, cifrados y firmas.

Esta complejidad no solo afecta a las prestaciones de los algoritmos, sino que también puede tener un impacto negativo en su seguridad. Por un lado, es más difícil entender los algoritmos y evaluar exhaustivamente la seguridad de su diseño desde el punto de vista **teórico**, lo que deja abierta la posibilidad de que los análisis criptográficos no logren identificar alguna vulnerabilidad o de que surjan nuevas técnicas de ataque a su base matemática. Por otro lado, las operaciones matemáticas involucradas en los algoritmos PQC son más complejas de **implementar**, lo que aumenta el riesgo de errores en las implementaciones, tanto *software* como *hardware*, que un adversario podría aprovechar para vulnerar los algoritmos o los protocolos criptográficos que los utilicen.

En los algoritmos PQC resulta complicado entender incluso los conceptos básicos de seguridad, como ocurre por ejemplo en el caso de los problemas relacionados con retículos. En este contexto, un problema de retículos P_a usado para construir un algoritmo criptográfico debe cumplir que resolver una instancia promedio suya resulte al menos tan difícil como resolver cualquier instancia del peor caso de otro problema de retículos relacionado P_w cuya seguridad ha podido ser demostrada. Esta propiedad se logra mediante reducciones matemáticas que garantizan que, si un adversario puede resolver eficientemente una instancia promedio de P_a , también podría resolver cualquier instancia del problema intratable P_w . Se ha demostrado, por ejemplo, que para $P_a = \text{LWE}$ el problema P_w puede ser SIVP o GapSVP en retículos euclideos generales, mientras que cuando $P_a = \text{M-LWE}$ el problema P_w correspondiente es SIVP restringido a retículos modulares [197] [198] [201] [228] [229].

Otro aspecto importante en relación con la seguridad de los esquemas post-cuánticos es el **equilibrio seguridad vs eficacia**. Como se vio en la sección anterior, en algunos algoritmos basados en retículos y en códigos se ha introducido estructura adicional al problema matemático base para que su rendimiento sea mejor y sus tamaños de clave, de encapsulado y de firma menores, tratando así de favorecer su adopción en la práctica. Sin embargo, añadir estructura a los retículos y códigos reduce el margen de seguridad de los esquemas respecto a los casos no estructurados y puede abrir la puerta a ataques algebraicos. En particular, CRYSTALS-KYBER reduce el margen de seguridad de FrodoKEM al usar retículos modulares en lugar de euclideos para el LWE, de la misma manera que BIKE y HQC reducen el margen respecto a Classic-McEliece al utilizar códigos con estructura, aunque no está claro si en estos casos la reducción implica un riesgo real para la seguridad de los algoritmos.

En lo que se refiere a la implementación, las operaciones matemáticas de los algoritmos PQC son complejas y, si no se implementan adecuadamente, pueden facilitar que un adversario pueda vulnerar su seguridad mediante **ataques de canal lateral**. Este tipo de ataque explota fugas de información involuntarias en la ejecución de un algoritmo para comprometer su seguridad, típicamente el tiempo de ejecución, el consumo de energía o la radiación electromagnética. Se han realizado ataques de canal lateral a diferentes implementaciones de muchos de los algoritmos KEM y DS propuestos en el concurso del NIST y, a su vez, se han propuesto contramedidas para mitigar las fugas de información [230] [231] [232] [233] [234] [235]. Las contramedidas más habituales son la ejecución en tiempo constante (para evitar que los bits de clave influyan en el tiempo de ejecución) y el enmascaramiento (que aleatoriza algunos datos sensibles durante las operaciones).

También cabe preguntarse si los algoritmos PQC desarrollados son realmente resistentes a la computación cuántica en general, y no solo a los algoritmos cuánticos conocidos hasta ahora. El **criptoanálisis cuántico** es un área incipiente, principalmente teórica al no disponerse de sistemas CRQC, pero que podría desarrollarse en los próximos años a medida que lo haga la computación cuántica. En abril de 2024, Chen publicó un complejo algoritmo cuántico con el que afirmaba ser capaz de resolver el problema LWE en tiempo polinomial en un CRQC, lo que pondría en jaque a muchos algoritmos basados en retículos como los estándares ML-KEM y ML-DSA. Sin embargo, había un error de concepto en el último paso del ataque que hace que no funcione, error que fue descubierto unos días después de la publicación por varios criptólogos [236] [237]. A pesar de ello, este trabajo supone un hito importante en el criptoanálisis cuántico de retículos e impulsará la investigación en esta disciplina.

Todo lo anterior ha generado **dudas** sobre el reemplazo de los algoritmos clásicos por post-cuánticos y está ralentizando la transición a PQC que se necesita para lograr resistencia cuántica en Internet. Además, es un hecho que muchos de los algoritmos participantes en el concurso PQC del NIST han sido vulnerados en estos últimos años. Según [238], hasta enero de 2024 se habían identificado vulnerabilidades del 48% de las propuestas de la primera ronda de evaluación y del 36% de las que avanzaron a la segunda ronda. Estos porcentajes elevados alimentan las suspicacias sobre la madurez de los algoritmos PQC y la urgencia con la que se desea abordar la transición. Preocupa especialmente que incluso algunos algoritmos que llegaron hasta las fases finales del concurso hayan sido atacados, como es el caso del encapsulamiento SIKE y de las firmas Rainbow y GeMSS.

Por ello, muchos expertos de la comunidad criptográfica [238] están apostando por una **aproximación híbrida** y la mayoría de las empresas tecnológicas punteras [239] [240] siguen también esta línea. El enfoque híbrido consiste en combinar un algoritmo clásico y otro post-cuántico para garantizar un determinado servicio de seguridad, de forma que un actor malicioso debe ser capaz de vulnerar ambos para llevar a cabo un ataque contra dicho servicio. Al mismo tiempo, también se está imponiendo la **cripto-agilidad** en los protocolos, es decir, la capacidad de cambiar los algoritmos criptográficos de forma sencilla para reemplazar aquellos que puedan llegar a comprometerse por otros que sigan siendo seguros, así como para tener la posibilidad de abandonar la hibridación en el futuro si aumenta la confianza en los algoritmos PQC.

La aproximación híbrida es una **opción conservadora** para empezar a abordar con garantías de seguridad la transición a la criptografía post-cuántica que proteja la información ante la eventual llegada de un CRQC. Al introducir gradualmente los algoritmos PQC mientras se mantienen los algoritmos clásicos, que han permanecido seguros durante décadas, se minimizan los riesgos derivados de potenciales fallos en el diseño o la implementación de primitivas PQC. De este modo es posible iniciar la transición post-cuántica sin correr el riesgo derivado de que en los próximos años alguno de los algoritmos PQC adoptados sea criptoanalizado [238] [240].

A pesar de esta ventaja de la criptografía híbrida, también presenta algunos inconvenientes. Sus detractores (entre ellos, la NSA [242]) argumentan que las construcciones híbridas añaden **complejidad** al diseño de los protocolos, ya que es preciso combinar adecuadamente las primitivas clásicas y post-cuánticas en juego, lo que amplía la superficie de ataque de los mismos. También aseguran que se incrementa el **coste computacional**, aunque el sobrecoste que supone añadir el algoritmo clásico al post-cuántico suele ser bastante pequeño en cuanto a longitud de los parámetros y moderado en lo que respecta al rendimiento en su ejecución.

Un caso práctico que subraya el valor estratégico de las construcciones híbridas en la transición fueron los experimentos llevados a cabo independientemente por Google y Cloudflare con TLS en 2016 y 2019 [238] [239] [240] [241]. Para estas pruebas, se implementaron acuerdos de claves que combinaban un algoritmo clásico (ECDH con curva elíptica X25519) con una primitiva post-cuántica (el KEM SIKE). A pesar de que SIKE fue vulnerado posteriormente, los datos transmitidos durante las pruebas continuarán estando protegidos gracias al ECDH clásico hasta que algún hipotético adversario que los haya almacenado tenga acceso a un CRQC.

5.5 Transición a firmas digitales post-cuánticas

A día de hoy existen ya algoritmos de firma digital en PQC que pueden utilizarse como **alternativa de las firmas clásicas** actuales, que típicamente se construyen con RSA, DSA o ECDSA. De hecho, el NIST ya ha estandarizado dos algoritmos de firma, CRYSTALS-DILITHIUM y SPHINCS+, y está desarrollando el estándar de un tercero, FALCON [180] [191] [193]. Desde el punto de vista de su adopción, es fundamental considerar las características específicas de cada algoritmo de firma para seleccionar el más adecuado según los requisitos de cada caso de uso.

En primer lugar, hay que tener en cuenta que las **longitudes de clave y firma** varían considerablemente de un algoritmo PQC a otro, y también con respecto a los algoritmos clásicos. En la Tabla 5-3 se pueden ver los tamaños de clave y de firma en algoritmos clásicos y post-cuánticos, parametrizados para el nivel de seguridad 1 (equivalente a un AES-128), excepto para CRYSTALS-DILITHIUM, cuyos parámetros corresponden al nivel 2 dado que no hay nivel 1 para este algoritmo. En el caso de SPHINCS+ se consideran dos alternativas, ‘s’ (*short*) y ‘f’ (*fast*); la variante ‘s’ genera una firma más corta que la ‘f’ pero menos eficientemente. En la tabla las filas correspondientes a algoritmos clásicos se han marcado en azul, y las de algoritmos PQC en naranja [243] [244].

Algoritmo	Cl. pública (bytes)	Cl. privada (bytes)	Firma (bytes)
RSA-3072	384	384	384
DSA-3072	384	320	56
ECDSA-256	64	32	64
DILITHIUM-2	1.312	2.528	2.420
FALCON-512	897	1.281	666
SPHINCS+-128f	32	64	17.088
SPHINCS+-128s	32	64	7.856

Tabla 5-3. Longitudes de clave y firma de algunos algoritmos de firma digital [243] [244].

Por otra parte, los **tiempos de ejecución** de las tres funciones que componen el esquema de firma digital (generación de clave, creación de firma y verificación de firma) también varían notablemente de unos algoritmos PQC a otros, como se puede ver en Tabla 5-4. Es habitual utilizar la librería en C de código abierto *Open Quantum Safe* (liboqs) [245] para medir prestaciones de algoritmos post-cuánticos en diferentes arquitecturas, pues no solo implementa la mayoría de los algoritmos que han participado en las fases finales del concurso NIST sino que además permite ejecutar *benchmarks*.

Cada valor de esta tabla se ha tomado directamente del artículo [244], y corresponde al tiempo medio (en microsegundos) de 100 iteraciones de la función correspondiente implementada en liboqs sobre un procesador Intel Core i7-9750H con 8 núcleos y frecuencia de reloj 2,6 GHz. En la medida de las operaciones de creación y verificación de firma, el tamaño del mensaje firmado es de 10 MB. Además, en el caso de la firma SPHINCS+, la función *hash* utilizada es SHA-256; el artículo referenciado muestra que el rendimiento de SPHINCS+ es del mismo orden si se utiliza SHAKE-256 en lugar de SHA-256.

Algoritmo	Genera clave (μs)	Genera firma (μs)	Verifica firma (μs)
DILITHIUM-2	500	25.920	37.840
FALCON-512	8.910	25.290	35.880
SPHINCS+-128f	700	52.230	27.090
SPHINCS+-128s	19.750	187.730	26.670

Tabla 5-4. Tiempo de ejecución de algunos algoritmos PQC de firma digital [244].

De acuerdo con estos datos, **SPHINCS+** resulta la opción menos recomendable para su uso en protocolos criptográficos, debido tanto al tamaño significativamente mayor de sus firmas en comparación con los otros algoritmos, como al elevado tiempo de ejecución de la función de generación de firmas. Incluso la variante ‘s’ resulta poco conveniente para este uso, pues, aunque genera firmas algo más cortas (aún mayores que las de DILITHIUM y FALCON), lo hace a costa de un sobre coste alto en las funciones de generación de clave y firma. SPHINCS+ es más adecuado para escenarios que requieren firmas esporádicas, como en contratos digitales o *firmware* de equipos electrónicos, donde las limitaciones de tamaño de firma y bajo rendimiento no suponen un problema.

Con respecto al uso de **CRYSTALS-DILITHIUM** y **FALCON** en protocolos, se puede observar en Tabla 5-3 y Tabla 5-4 que ambos algoritmos tienen un coste similar en términos de generación y verificación de firmas, pero que CRYSTALS-DILITHIUM es bastante más eficiente que FALCON en cuanto a la generación de claves (casi 20 veces más rápido). Por otro lado, FALCON es capaz de generar claves y firmas más pequeñas, lo que lo hace apropiado para protocolos con limitaciones de tamaño de firma o ancho de banda, como en dispositivos IoT, sistemas embebidos o *blockchain*, donde la eficiencia en el uso de recursos es crítica y la lentitud del proceso de generación de claves no es un factor crítico.

Debido al carácter más general de CRYSTALS-DILITHIUM, junto con el hecho de que ya se ha sido estandarizado como ML-DSA en FIPS 204, este algoritmo se ha convertido en la opción PQC más utilizada para firmas digitales en la transición post-cuántica de los protocolos criptográficos. Sin embargo, en lugar de depositar confianza plena en los nuevos algoritmos PQC, cuya seguridad aún requiere mayor escrutinio por parte de la comunidad científica y pruebas rigurosas de las implementaciones específicas, la opción más extendida está siendo adoptar **firmas digitales híbridas**, en las que se combina el algoritmo ML-DSA con otro algoritmo clásico como mecanismo de seguridad adicional durante la transición [246][250].

La aproximación para la hibridación propuesta en el borrador *draft-ietf-lamps-pq-composite-sigs-03* del IETF [246], en el que colaboran activamente expertos de Entrust, OpenCA y Cisco, entre otros, consiste en generar una firma combinada compuesta por **dos firmas independientes**: una con ML-DSA y otra con un algoritmo clásico (RSA, ECDSA, Ed25519 o Ed448). Esta firma combinada ha sido definida para integrarse en los estándares X.509 [51] para certificados digitales, PKIX [247] para la infraestructura de clave pública y CMS [248] con la sintaxis habitual de mensajes criptográficos que emplean los anteriores, que son ampliamente utilizados en el Internet actual. Cuando FALCON sea estandarizado, es muy posible que su longitud de firma, menor que la de ML-DSA, se impulse su uso como componente post-cuántico del esquema de doble firma.

Por otra parte, se está investigando sobre cómo combinar los dos algoritmos de firma, clásico y post-cuántico, más allá de su simple agregación o concatenación, con el objetivo de reducir la longitud de la firma generada manteniendo su seguridad [249] [250]. Sin embargo, la reducción lograda hasta ahora es limitada, principalmente porque la longitud de la firma PQC es el factor dominante, superando en uno o dos órdenes de magnitud la longitud de la firma clásica. Por ejemplo, en la combinación ECDSA con curva P-256 y FALCON-512, la agregación directa genera firmas de 730 bytes (64 de ECDSA y 666 de FALCON), mientras que el esquema reducido propuesto en [250] genera firmas de 698 bytes, solo un 4,38% más cortas. Dado que la reducción es pequeña, es razonable esperar que, al menos en los primeros años de transición post-cuántica, se apueste por una simple agregación de las dos firmas, ya que esta opción resulta más sencilla.

5.6 Transición a encapsulamientos de clave post-cuánticos

Como se ha visto en las secciones anteriores, ya existen algoritmos KEM que pueden ser utilizados para el establecimiento de claves en protocolos criptográficos, dotándolos de resistencia frente a ataques cuánticos. El instituto NIST ha estandarizado CRYSTALS-KYBER (ML-KEM) [191] y continua evaluando tres esquemas basados en códigos de corrección de errores, Classic-McEliece, BIKE y HQC, con el objetivo de estandarizar uno de ellos a corto plazo [190]. El algoritmo basado en isogenias de curva elíptica SIKE, que NIST valoraba como alternativa a los anteriores, ha sido vulnerado recientemente, quedando fuera del proceso de evaluación [224].

A pesar de la disponibilidad de un estándar KEM basado en retículos, otros algoritmos de esta familia siguen siendo relevantes. En algunos casos, no se considera adecuada la reducción del margen de seguridad que supone utilizar M-LWE en lugar de LWE para ganar en eficiencia, y se prefiere optar por FrodoKEM como opción más conservadora (una recomendación, por ejemplo, del BSI [208]). Por otro lado, algunos protocolos criptográficos comenzaron a implementar otros algoritmos de KEM antes de que el NIST anunciara su decisión de promover y estandarizar CRYSTALS-KYBER, como es el caso de SSH con NTRU-Prime [251].

Tal y como ocurre con las firmas digitales, tanto las **longitudes de clave y encapsulado** como los **tiempos de ejecución** de las funciones del KEM (generación de clave, encapsulado y desencapsulado) varían considerablemente de un algoritmo a otro, lo que motiva que la elección de un KEM concreto sea muy dependiente del caso de uso en el que se vaya a aplicar o de posibles restricciones de la arquitectura en la que se pretenda implementar. En la Tabla 5-5 se muestran los parámetros de los principales algoritmos de KEM basados en retículos y códigos para el nivel de seguridad 1 (excepto NTRU-Prime, cuya parametrización básica es nivel 2), y además los de los algoritmos clásicos RSA-3072 y ECDH con curva X25519 para facilitar la comparativa [204] [202] [205] [211] [212] [213].

Algoritmo	Cl. pública (bytes)	Cl. privada (bytes)	Encapsulado (bytes)
RSA-3072	384	384	N/A
ECDH-X25519	32	32	N/A
FrodoKEM-640	9.616	19.888	9.720
KYBER-512	800	1.632	768
NTRULPR-761	1.039	1.328	1.167
CI-McEliece-348864	261.120	6.492	96
BIKE-L1	1.540	280	1.572
HQC-128	2.249	2.289	4.497

Tabla 5-5. Longitudes de clave y cifrado de algoritmos KEM (según especificaciones).

Se puede comprobar que el tamaño de clave pública de los KEM aumenta respecto al de los algoritmos de clave pública clásicos, y que este aumento es más moderado en el caso de retículos que en el de códigos, destacando la enorme clave pública que requiere Classic-McEliece. También se observa que las instancias con estructura de los problemas de retículos y códigos reducen significativamente el tamaño de las claves, haciendo que los algoritmos sean más prácticos que los basados en las instancias generales. Por otro lado, el tamaño de los cifrados en los algoritmos post-cuánticos aumenta aproximadamente en una proporción similar al de las claves públicas, salvo en el caso de Classic-McEliece, donde el tamaño del cifrado es considerablemente más pequeño.

En la Tabla 5-6 se indican los tiempos de ejecución de las tres funciones de los KEM anteriores, obtenidos de los *benchmarks* de liboqs para arquitecturas x86_64 [245] [252]. Los más rápidos en las operaciones de encapsulado y desencapsulado son KYBER-512 y NTRULPR-761, destacando el primero en la generación de claves, y el más costoso es FrodoKEM-640. Classic-McEliece es también muy eficiente encapsulando y desencapsulando, bastante mejor que BIKE-L1 y HQC-128, aunque el rendimiento de su generación de claves es muy pobre.

Algoritmo	Genera clave (μ s)	Encapsula (μ s)	Desencapsula (μ s)
FrodoKEM-640	1.342	1.512	1.483
KYBER-512	12	15	11
NTRULPR-761	416	20	23
CI-McEliece-348864	54.945	20	48
BIKE-L1	255	44	700
HQC-128	42	79	144

Tabla 5-6. Tiempo de ejecución de algunos algoritmos KEM [252].

En cuanto al rendimiento respecto de los algoritmos clásicos, en [253] se comparan las operaciones de KYBER-512 (encapsulado) con las de RSA-2048 (cifrado) y ECDH-X25519 (acuerdo de clave). En cuanto a la generación de claves, la de KYBER-512 es considerablemente más rápida que la de RSA-2048 (con un factor ~ 4.167) y también es algo más rápida que la de X25519 (un factor ~ 1.56), aun siendo esta curva elíptica de las más eficientes en uso. Por otro lado, el encapsulado de KYBER-512 es algo más ineficiente que el de RSA-2048 (~ 0.5 veces más lento), pero su desencapsulado es bastante más rápido (un factor ~ 71.43).

No es posible comparar directamente el rendimiento de las funciones de encapsulado y desencapsulado de un KEM con las funciones involucradas en un acuerdo de claves DH o ECDH, pues su uso criptográfico no es equivalente. En la siguiente sección se tratará sobre cómo se construyen **esquemas de establecimiento de claves basados en KEM**, para su uso en protocolos criptográficos y se abordará el impacto en prestaciones que tiene incorporar este tipo de esquemas en los protocolos habituales, como por ejemplo IKE, TLS o SSH. Se verá también que lo más habitual es emplear **esquemas híbridos**, combinando los basados en KEM con ECDH clásicos, como solución conservadora ante la posibilidad de que los KEM implementados sean vulnerados durante el proceso de transición.

Finalmente, es importante señalar que la **transición hacia la criptografía post-cuántica**, tanto en los algoritmos de KEM como en los de DS, no ha hecho más que empezar. Como se ha visto en esta sección, en los últimos años ha habido un avance notable en el desarrollo de algoritmos PQC, y aunque algunos ya han sido estandarizados, los procesos de evaluación y estandarización siguen en curso. Ya ha empezado a abordarse cómo integrar las nuevas primitivas PQC en los protocolos criptográficos y, en algunos casos, a implementar estas soluciones. Sin embargo, aún queda un largo camino por recorrer hasta que los nuevos algoritmos logren desplazar completamente a los algoritmos de clave pública vulnerables a la computación cuántica.

Es de esperar que la transición será un **proceso largo, complejo y costoso**. Resulta representativo el informe [254], presentado recientemente por la administración de EEUU a su gobierno, que indica la necesidad de empezar la migración hacia PQC antes de la posible aparición de un CRQC por el riesgo que supone el ataque ‘cosecha-ahora-descifra-después’, y propone una estrategia de migración. Esta estrategia comienza con el inventario de los sistemas criptográficos en uso, para posteriormente priorizar cuáles requieren protección más urgente e identificar aquellos que no pueden ser migrados (cuyo riesgo deberá mitigarse con soluciones alternativas). El informe estima un coste de aproximadamente 7.100 millones de USD para llevar a cabo la migración entre 2025 y 2035.

En la sección 6.4 se muestran algunos ejemplos de protocolos criptográficos que han comenzado a integrar los algoritmos post-cuánticos de KEM.

6 RESISTENCIA CUÁNTICA EN PROTOCOLOS IP

Esta sección resume lo visto hasta ahora sobre la amenaza que representa la computación cuántica para las primitivas y protocolos criptográficos utilizados en las comunicaciones IP y las soluciones que se están desarrollando para conseguir dotar de resistencia cuántica a la autenticación de las partes y el establecimiento de la clave de sesión en los protocolos.

Se describen tres enfoques para conseguir esta resistencia cuántica: el uso de criptografía simétrica, la implementación de comunicaciones cuánticas y la adopción de algoritmos de criptografía post-cuántica. En cada caso, se presentan las ventajas asociadas a su aplicación, así como las limitaciones que plantean en términos de adopción y compatibilidad con la infraestructura actual de Internet. Además, se detallan las implementaciones prácticas y estándares relacionados con cada una de estas aproximaciones en los protocolos criptográficos más relevantes.

6.1 Amenaza cuántica a los protocolos criptográficos

Como se explica en la sección 3, la **amenaza cuántica** pone en riesgo la criptografía actual y, en consecuencia, los protocolos criptográficos que se construyen usando estas primitivas para garantizar la seguridad de la información que se transmite por Internet. Los avances en el desarrollo de la computación cuántica cada vez acercan más la construcción de un CRQC, capaz de resolver algunos problemas matemáticos que fundamentan la seguridad de los algoritmos actuales. A pesar de que las previsiones más optimistas no esperan que pueda construirse un CRQC antes de una década, es importante empezar a considerar seriamente la amenaza que representa.

Existen algoritmos cuánticos teóricos para resolver la factorización entera y el logaritmo discreto en campos finitos en un CRQC en tiempo polinomial (Shor y variantes optimizadas), lo que reduciría drásticamente la seguridad de los algoritmos de clave pública que se usan actualmente en muchos protocolos criptográficos, típicamente RSA, DSA, DH, ECDH, ECDSA y EdDSA. Como se describió en la sección 2.4, estos algoritmos se utilizan en la primera fase de los protocolos criptográficos para la autenticación de las partes y el establecimiento de la clave de sesión, de modo que **la fase 1 de los protocolos criptográficos está amenazada**.

Por otra parte, en la segunda fase de los protocolos criptográficos las partes intercambian mensajes cifrados y autenticados con claves derivadas de la clave de sesión establecida, y para ello solo utilizan algoritmos de cifrado simétricos y funciones MAC. A día de hoy, el único algoritmo cuántico teórico que mejora las capacidades de computación clásicas es el de Grover, que haría más eficiente los ataques por fuerza bruta a estas primitivas. En la práctica, la seguridad de un algoritmo simétrico de longitud de clave L quedaría reducida a $L^{1/2}$ ante un CRQC capaz de ejecutar el algoritmo de Grover, de manera que puede garantizarse su resistencia cuántica siempre y cuando L sea suficientemente grande.

La máxima longitud de clave que utilizan los algoritmos simétricos actuales es de 256 bits, lo que garantizaría un nivel de seguridad de 128 bits frente a un adversario con un CRQC tras aplicar la reducción cuadrática del algoritmo de Grover, un nivel que se considera suficientemente seguro. Sin embargo, algoritmos simétricos con claves de 128 bits o inferiores verían reducido su nivel de seguridad a 64 bits o menos, un margen de seguridad computacional insuficiente. En consecuencia, **la fase 2 de los protocolos criptográficos no está amenazada** si se utilizan algoritmos simétricos robustos, correctamente implementados y con claves de longitud suficiente.

Los esquemas AES-GCM, AES-CCM y CHACHA20-POLY1305 de AEAD, presentados en la sección 2.6, garantizarían un nivel de seguridad de 128 bits frente a un CRQC siempre y cuando la clave empleada para AES o CHACHA20 tenga longitud de 256 bits. Estos esquemas ya se utilizan en los protocolos criptográficos más empleados en Internet, como se muestra en la Tabla 2-1. Resulta posible, además, conseguir niveles de seguridad mayores de 128 bits tras la reducción de Grover, bien utilizando algoritmos simétricos con claves más largas (por ejemplo, Threefish, que usa claves de 512 bits) o bien utilizando varios algoritmos como AES o CHACHA20 en cascada.

En los apartados que siguen, se pone el foco en cómo garantizar la resistencia cuántica de la primera fase de los protocolos criptográficos, en la cual las partes se autentican y establecen claves de sesión (AKE), y se da por hecho que la segunda fase de los mismos es resistente.

6.2 Resistencia cuántica con criptografía simétrica

Dado que la criptografía simétrica muestra una mayor resiliencia frente a la amenaza cuántica que la de clave pública, una forma directa de garantizar la resistencia cuántica es utilizar protocolos criptográficos en los que la autenticación de las partes y el establecimiento de la clave de sesión (AKE, por sus siglas en inglés) se realicen exclusivamente mediante primitivas simétricas. De este modo, **se evitan los algoritmos de clave pública** vulnerables a la eventual llegada de un CRQC capaz de resolver en tiempo polinomial los problemas matemáticos de factorización y logaritmo discreto.

Como se explicó en la sección 2.5, existen dos tipos de AKE contruidos con criptografía simétrica, los que se basan en claves pre-compartidas directamente entre los comunicantes y los que utilizar una tercera parte de confianza en línea como intermediaria; en este último caso, cada parte comparte un secreto con la TTP. La principal limitación de estas dos aproximaciones es que los comunicantes, y la TTP si participa en el protocolo, tienen que **acordar los secretos por un canal auxiliar**. Este canal auxiliar debe ser confidencial, ya que la seguridad del AKE depende completamente de que estos secretos no sean comprometidos. Un adversario que comprometiera la clave pre-compartida de una de las partes podría recuperar sus claves de sesión e incluso llegar a suplantarla.

Cuando no hay una TTP, las partes deben compartir directamente entre sí las PSK correspondientes, en función de las cuales se autenticarán y establecerán claves de sesión en el AKE. Este enfoque **limita considerablemente la usabilidad y la escalabilidad** de este tipo de soluciones, por lo que su en la práctica se limitan a entornos cerrados, con pocos usuarios y con relaciones de confianza previamente establecidas entre ellos (se requiere, además, un canal auxiliar seguro de distribución de PSK mencionado anteriormente). Estos protocolos no resultan prácticos para su uso en aplicaciones masivas, distribuidas o globales de Internet. Sin embargo, existen AKE de este tipo en protocolos genéricos como IPSEC y TLS, como opción orientada a para redes pequeñas, y también en protocolos de acceso remoto a servidores (SSH) y de conexión inalámbrica (WPA2, WPA3, Bluetooth, etc.).

En el caso particular de **IPSEC**, esta aproximación ha sido adoptada en los últimos años por importantes fabricantes, tales como Cisco, Fortinet o Checkpoint, para dotar de resistencia cuántica a sus equipos **añadiendo claves pre-compartidas al protocolo IKEv2** conforme a lo especificado en el RFC 8784 [255]. La inclusión de PSK en IPSEC no solo garantiza la **confidencialidad** de las claves de sesión frente a un adversario con capacidades cuánticas avanzadas, sino que además aportan un mecanismo de **autenticación mutua** entre las partes, ya que únicamente los comunicantes legítimos conocen los secretos pre-compartidos. Incluso en escenarios donde IKEv2 utilice una PKI clásica cuya seguridad podría verse comprometida por un adversario cuántico, las PSK siguen garantizando la autenticación de las partes.

Los cambios introducidos por **RFC 8784** en IKEv2 son mínimos: las partes comparten un conjunto de PSK, acuerdan durante la negociación inicial cuál de ellas usar y, finalmente, integran la PSK seleccionada en el método tradicional de autenticación y establecimiento de claves de IKEv2. En concreto, si SK representa la clave de sesión que acuerdan las partes por métodos clásicos (por ejemplo, ECDH) y PSK es la clave pre-compartida que negocian, la clave de sesión de la SA (*Security Association*) principal del IKE se deriva como:

$$\begin{aligned} \text{PRF}^+(\kappa, v) &:= \text{HMAC}(\kappa, v \parallel 0x01) \parallel \\ &\quad \text{HMAC}[\kappa, \text{HMAC}(\kappa, v \parallel 0x01) \parallel v \parallel 0x02] \parallel \dots \\ \text{SKEYSEED} &= \text{HMAC}(\text{nonces}, \text{ecdh_secret}) \\ \text{SK} &= \text{PRF}^+(\text{SKEYSEED}, \text{nonces} \parallel \text{ids}) \\ \text{SK}^* &= \text{PRF}^+(\text{PSK}, \text{SK}) \end{aligned}$$

donde PRF^+ es la función pseudo-aleatoria utilizada en IKEv2 para derivación de claves y el HMAC emplea SHA-2 o SHA-3 como función hash subyacente [14] [255]. Por las propiedades de la función PRF^+ , un adversario no puede recuperar SK^* si solo conoce una de las claves que se combinan.

Como se analizará en la sección 6.4, tras la reciente aprobación por parte del NIST de los primeros algoritmos de clave pública post-cuánticos, los fabricantes de equipos IPSEC han comenzado a implementarlos como solución post-cuántica. Ahora bien, el uso de PSK sigue siendo aplicable en este contexto para entornos cerrados, con la única diferencia de que la clave de sesión SK se genera en este caso añadiendo secretos transportados con KEM post-cuánticos (como se explicará en la sección 6.4). Por otra parte, es interesante destacar que otros protocolos criptográficos también permiten integrar una clave pre-compartida en su AKE clásico tal y como hace IPSEC, como es el caso de **WIREGUARD** [12] y **TLSv1.3** [19].

En el contexto de protocolos criptográficos con AKE basados en criptografía simétrica en los que intermedia tercera parte, la TTP es típicamente un servidor de claves que debe estar en línea. Kerberos es el ejemplo más representativo de este tipo de protocolo. En este caso, además del problema que supone la necesidad de un canal auxiliar para que las partes compartan sus PSK con el servidor para autenticarse ante él y que este pueda distribuir claves de sesión dinámicamente, existen otras limitaciones. En primer lugar, el servidor debe ser capaz de gestionar de manera eficiente las solicitudes de los participantes de la red, lo que puede resultar complicado si hay un gran número de usuarios, por lo que la TTP es un **cuello de botella** en términos de escalabilidad y rendimiento. Por otro lado, la dependencia del servidor de claves introduce un **punto único de fallo**, ya que la seguridad queda completamente comprometida si un adversario es capaz de vulnerar el servidor y obtener la base de datos de PSK que gestiona.

En conclusión, aunque los AKE basados únicamente en criptografía simétrica ofrecen una solución robusta frente a la amenaza cuántica, al evitar algoritmos de clave pública, su aplicabilidad está limitada a redes con un número reducido de usuarios, en las que las relaciones de confianza ya están establecidas. Esto se debe a la necesidad de establecer canales auxiliares seguros que aseguren la correcta distribución previa de PSK, tanto si se utiliza una TTP en línea para servir las claves de sesión como si no. Además, este tipo de protocolo no ofrece secreto hacia adelante, como se explicó en la sección 2.5. Aunque estos protocolos pueden ser adecuados para **redes de pocos usuarios con confianza mutua**, e incluso en **entornos corporativos**, no resultan prácticos en un escenario global como el de Internet, donde la distribución segura de claves pre-compartidas puede ser inabordable.

6.3 Resistencia cuántica con comunicaciones cuánticas

En la sección 4 se analiza la posibilidad de utilizar claves aleatorias transmitidas a través de un canal cuántico, típicamente fotónico, como medio para resistir a la amenaza de un CRQC. Por las propiedades cuánticas del canal, ningún adversario puede copiar los bits de clave que se transmiten sin que las partes detecten la intrusión y descarten dichos bits. Además, si las claves compartidas por QKD son aleatorias, de un solo uso y se emplean para cifrar mensajes de menor longitud con *One Time Pad*, este mecanismo permite a priori construir un criptosistema con seguridad incondicional (sección 2.3).

A pesar de su potencial para garantizar resistencia cuántica, esta tecnología presenta importantes **limitaciones que dificultan la adopción de QKD en una red global como Internet**. Algunas de estas limitaciones están relacionadas con la propia naturaleza de los sistemas cuánticos (sección 4.3), como la reducida distancia a la que se pueden establecer enlaces y las bajas tasas de generación de claves alcanzadas, mientras que otras se refieren a aspectos de su implementación. Es esta última categoría destacan: la necesidad de equipos específicos e infraestructura dedicada, las vulnerabilidades en las implementaciones, la sensibilidad a ataques de DoS, la necesidad de canal auxiliar para la autenticación de las partes y el post-procesado de la señal fotónica, y falta de madurez de la tecnología y de los estándares necesarios para garantizar la interoperabilidad entre sistemas (sección 4.7).

Son estas limitaciones las que han llevado a instituciones clave, como la NSA, el BSI, el NCSC y el ANSSI, a recomendar en los últimos años el uso de criptografía post-cuántica en lugar de QKD para lograr resistencia cuántica en Internet. No obstante, estas instituciones han dejado la puerta abierta al **empleo de QKD en casos específicos** en los que se desee proporcionar un nivel adicional de seguridad a las comunicaciones que justifique la elevada inversión necesaria para su implementación. En este contexto, se están desarrollando diversos proyectos de QCI que interconectan varios nodos QKD para crear redes de comunicaciones de mayor envergadura (sección 4.5), principalmente infraestructuras terrestres (MadQCI) y, en menor medida, satelitales (Micius).

Debido al limitado alcance de la señal fotónica, y puesto que aún no se han desarrollado repetidores cuánticos capaces de llevar esta señal más lejos sin alterarla, el despliegue de una QCI a día de hoy utiliza como nodos de la red **repetidores clásicos**, capaces tanto de establecer enlaces QKD con otros nodos como de proveer de claves transmitidas por QKD a las aplicaciones que se lo demanden (sección 4.6). En cada nodo el KM (*Key Manager*) controla la generación continuada de claves QKD con los nodos con los que conecta y el ciclo de vida de estas claves, siendo además responsable de gestionar cómo las aplicaciones las consumen. Cada nodo tiene que ser confiable para los elementos de la red, dado que conoce las claves QKD que genera y suministra a las aplicaciones.

Las implementaciones de cifrado basado en claves generadas con QKD realizadas hasta ahora no han buscado alcanzar la seguridad incondicional que garantiza *One Time Pad*, sino la usabilidad que supone su integración en protocolos criptográficos existentes, pues de esta forma se simplifica la gestión de claves y se evita el impacto en la eficiencia de la limitada tasa de generación de QKD. De hecho, los equipos disponibles capaces de solicitar claves a dispositivos QKD son enrutadores que implementan **IPSEC**, como Cisco [256] o Fortinet [257]. Esta misma lógica sería fácilmente adaptable a otros protocolos criptográficos modernos como MACSEC en la capa de enlace, WIREGUARD en la capa de red y TLSv1.3 en la capa de transporte, ya que estos ya admiten la opción de uso de PSK.

En este caso de uso, cada equipo IPSEC solicita claves al KM de un nodo en una red QKDN y las utiliza para **reforzar las claves de sesión** que deriva en el IKEv2 clásico. De este modo, se construye un esquema híbrido que se beneficia de la resistencia cuántica que aportan las claves distribuidas cuánticamente a la vez que mantiene la interoperabilidad con otros equipos conectados en red. Además, si el empleo de claves QKD es opcional, los equipos IPSEC pueden seguir funcionando con claves derivadas clásicamente en el caso de que el sistema QKD no se encontrara disponible o que no proporcionara las claves a la velocidad que se le requieren.

Con este mecanismo se garantiza resistencia cuántica a la vez que se superan las principales limitaciones que tiene el empleo de PSK: la necesidad de un canal confiable por el que distribuir las claves, el coste a nivel de administración de la red para abordar esta distribución (sobre todo cuando aumenta el número de usuarios en la red) y la falta de secreto hacia adelante al reutilizar una misma clave simétrica para varias sesiones. Al igual que el uso de PSK, las claves QKD garantizan tanto la **confidencialidad** de las claves de sesión como la **autenticación de las partes** frente a potenciales adversarios cuánticos. Además, las claves distribuidas mediante QKD proporcionan **secreto hacia adelante** siempre y cuando sean efímeras, es decir, si se utilizan para una única sesión y no se guardan una vez derivada la SK final, comportamiento habitual de este tipo de soluciones.

Un ejemplo de integración de claves QKD en IPSEC es la extensión **SKIP** (*Secure Key Integration Protocol*) definido por Cisco [256]. Este estándar no se limita a QKD, sino que aborda el caso más general de contar con un proveedor externo de claves simétricas en línea para fortalecer IPSEC, aunque su uso más destacado es precisamente cuando este proveedor es un KM en una QKDN. Las claves QKD se obtienen dinámicamente, una para cada sesión, y no se necesita un canal auxiliar seguro para que las partes compartan secretos antes de comunicarse. La derivación de la clave de sesión en SKIP es similar a la del RFC 8784 para claves simétricas pre-compartidas, sustituyendo el uso de estas últimas por el de las claves QKD que suministra el KM. Con la notación del apartado anterior, la clave de sesión se calcula como $SK^* = \text{PRF}^+(QK, SK)$, siendo QK una clave QKD y SK la clave de sesión que acuerdan las partes por métodos clásicos.

En la Figura 6-1 se muestra la arquitectura de red en IPSEC con SKIP, así como el mecanismo de acuerdo de la clave simétrica con el proveedor externo. En SKIP en lugar de seguir el estándar ETSI GS-QKD-014 definido para tal fin, se define un protocolo propio basado en TLS, lo que refuerza la idea expuesta en la sección 4 sobre la falta de madurez de los estándares y problemas de interoperabilidad y escalabilidad que se derivan de ello. Como se resalta en rojo en la figura, el cifrador IPSEC que inicia la comunicación obtiene de su KM una clave QKD y un identificador de la misma durante el proceso IKEv2 y transmite este identificador al cifrador destino, que le solicita a continuación la correspondiente clave a su respectivo KM.

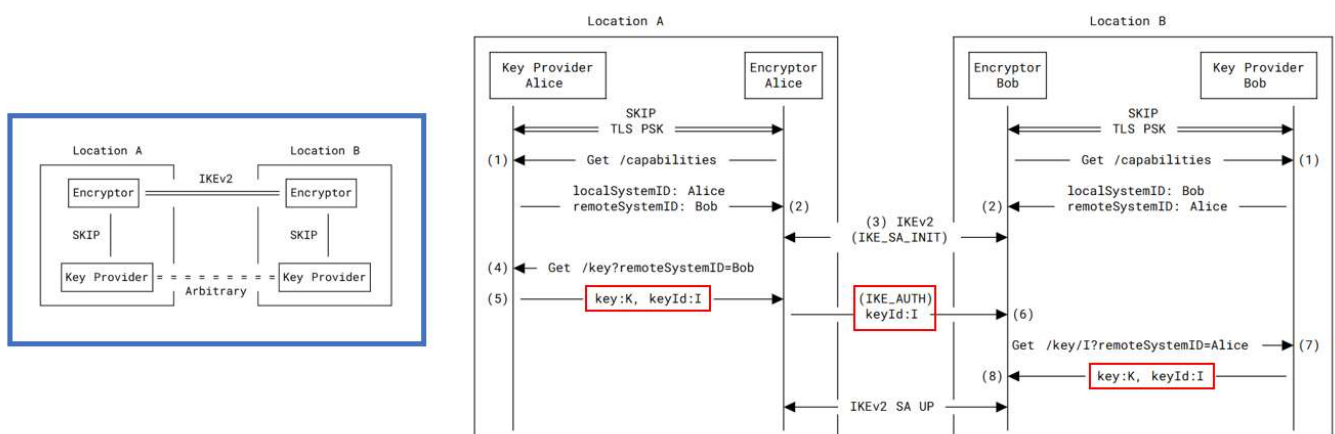


Figura 6-1 Arquitectura de red (izquierda) y acuerdo de clave (derecha) en SKIP [256].

6.4 Resistencia cuántica con criptografía post-cuántica

Como se ha justificado en los apartados anteriores, las soluciones basadas en criptografía simétrica y en comunicaciones cuánticas pueden ser útiles para garantizar la seguridad en redes con un número limitado de usuarios, pero no para su **uso generalizado en Internet**. Los servicios web, la nube, la mensajería instantánea, las redes sociales, el *streaming*, los juegos en línea, etc. tienen un gran número de usuarios, y la gestión de claves simétricas o el despliegue infraestructura de comunicaciones cuánticas para conectarlos en red de forma eficiente y segura resulta inviable. La criptografía de clave pública juega un papel fundamental en estos casos y, por ello, **es necesario abordar la transición hacia los nuevos algoritmos post-cuánticos** que garanticen la seguridad de este tipo de aplicaciones frente a un futuro adversario cuántico.

En la sección 5 se presentaron los algoritmos post-cuánticos que se han desarrollado y evaluado en los últimos años, tanto para encapsulamiento de claves (**KEM**) como para firma digital (**DS**), y se analizó el grado de madurez de los mismos, destacando el hecho de que recientemente el NIST haya aprobado los primeros estándares PQC tanto para KEM como para DS. En cuanto a la inclusión de estos algoritmos en la fase AKE de los protocolos criptográficos de Internet, los algoritmos KEM permiten implementar mecanismos para establecer claves de sesión, tal y como se hace clásicamente con DH y ECDH, mientras que los algoritmos DS post-cuánticos permiten la autenticación de las partes de forma similar a sus análogos clásicos.

Respecto a la transición post-cuántica, lo primero que hay que destacar es que la incorporación de KEM y DS a los protocolos criptográficos marcha a distinta velocidad, siendo **mucho mayor el esfuerzo que los expertos están dedicando a añadir los KEM**. La razón es que resulta más urgente garantizar la confidencialidad de las claves de sesión frente a un actor malicioso que implemente el ataque ‘cosecha-ahora-descifra-después’ y que pueda empezar a guardar ya sesiones para su futuro descifrado. Por otra parte, mientras no exista un CRQC, no podrán comprometerse las firmas digitales clásicas usadas en la actualidad (los ataques de suplantación han de ocurrir en el momento en el que se produce la comunicación), por lo que el uso de firmas digitales post-cuánticas no resulta una preocupación inmediata para la comunidad científica.

Como se explicó en la sección 5.5, se ha comenzado a investigar cómo construir **firmas digitales híbridas**, que combinen un algoritmo clásico y otro post-cuántico, con el objetivo de integrarlas en las infraestructuras PKI [51] [246] [248]. Además, recientemente se han publicado propuestas concretas para incorporar firmas híbridas en los protocolos IPSEC y TLSv1.3 [258] [259]. Por el momento, la opción más aceptada consiste en firmar digitalmente con ambos algoritmos de forma independiente y crear una firma combinada mediante la concatenación de las dos firmas. Aunque este enfoque añade resistencia cuántica a la vez que garantiza la compatibilidad con las infraestructuras actuales, tiene gran impacto en los protocolos criptográficos al aumentar notablemente tanto el tamaño de las firmas como el coste computacional de su generación y verificación.

La firma post-cuántica que se está considerando es CRYSTALS-DILITHIUM, pues su estándar ya está aprobado por el NIST (ML-DSA) y el coste de sus funciones de firma y verificación es razonable. El otro estándar disponible, SPHINCS+ (SLH-DSA), no se considera adecuado para protocolos IP porque tanto el tamaño de la firma que genera como el coste de la función de firma son muy elevados. Por otro lado, se espera que FALCON, el tercer algoritmo ganador del concurso del NIST pendiente de ser estandarizado, también se utilice en firmas híbridas porque genera claves y firmas más pequeñas que ML-DSA (sección 5.5). En lo que sigue, se centra la atención en la transición post-cuántica de los mecanismos de establecimiento de clave en los protocolos de Internet, mucho más avanzada que la incorporación de firmas digitales post-cuánticas.

Lo primero a destacar en cuanto al uso de KEM post-cuánticos en protocolos AKE es que, en la mayoría de los casos, el enfoque seguido es híbrido. Es decir, **se añade el transporte de clave basado en un KEM al acuerdo de clave clásico** (DH o ECDH, típicamente), combinando el secreto transportado con la clave acordada para derivar la clave de sesión. Este enfoque híbrido permite dotar de resistencia cuántica a los protocolos, a la vez que mantiene la compatibilidad con los algoritmos clásicos en uso, lo que facilita una transición progresiva. Además, **reduce el riesgo asociado a reemplazar directamente el acuerdo clásico maduro por un KEM que aún está bajo escrutinio**, especialmente teniendo en cuenta que algunos algoritmos KEM post-cuánticos ya han sido vulnerados, como SIKE [224].

Sin embargo, la aproximación híbrida para el establecimiento de claves presenta también ciertos inconvenientes que hacen que la transición sea compleja. Al añadir un KEM al AKE, **su implementación resulta más compleja** y, por tanto, más propensa a contener errores y vulnerabilidades que puedan ser aprovechadas por un adversario. Además, **el rendimiento se ve penalizado**, ya que aumenta el ancho de banda que se requiere para que las partes intercambien las claves públicas y los encapsulados durante el AKE, así como el tiempo de cálculo necesario para derivar la clave de sesión. Estas limitaciones son delicadas en redes con restricciones de ancho de banda o con dispositivos con recursos computacionales limitados (sistemas embebidos o dispositivos IoT), pues pueden provocar congestión en los canales de comunicación, aumentar la latencia en el establecimiento de conexiones y, en casos extremos, hacer inviables aplicaciones en tiempo real.

Se está incorporando este enfoque híbrido en el establecimiento de claves en protocolos fundamentales de Internet como **IPSEC** y **TLSv1.3**, así como en muchos otros en la capa de aplicación, entre los que cabe destacar SSH, SIGNAL (PQXDH) y PQ3. En el caso de **SSH**, la implementación de código abierto del protocolo OpenSSH incluye la posibilidad de combinar X25519 como algoritmo clásico con el encapsulamiento NTRU-Prime [251]; además, existe un *fork* de OpenSSH que permite utilizar diferentes algoritmos de la librería *liboqs* [260] [261]. La aplicación de mensajería Signal ha incorporado el establecimiento de claves híbrido **PQXDH** [262], una evolución del protocolo X3DH [263] que forma parte del protocolo de cifrado extremo a extremo también denominado SIGNAL por dicha aplicación. También la aplicación iMessage de mensajería instantánea nativa de Apple ha implementado un algoritmo con AKE híbrido, el **PQ3** [264].

Una excepción notable del enfoque híbrido generalizado es WIREGUARD, aplicación nativa del sistema operativo Linux para crear redes privadas virtuales, que implementa como protocolo criptográfico una instancia del conjunto de protocolos Noise, con claves públicas LTK pre-compartidas y EK para garantizar secreto hacia adelante. En este caso, no se ha planteado la hibridación del AKE, sino una revisión completa del protocolo basado exclusivamente en primitivas post-cuánticas, conocida como **PQ-WIREGUARD** [265] (también se ha propuesto una alternativa puramente post-cuántica de todo Noise en términos similares [266]). Esto se debe a que WIREGUARD carece de cripto-agilidad, pues en su diseño se favorecieron simplicidad y eficiencia, y no es posible seleccionar algoritmos distintos a los pre-establecidos. En este caso la transición será más costosa, pues no hay forma de introducir gradualmente los KEM, y se podrán producir problemas de compatibilidad entre versiones.

Para concluir la sección, se describe la implementación híbrida de los protocolos criptográficos IPSEC y TLSv1.3, que son fundamentales en el Internet actual para garantizar la seguridad de las comunicaciones en las capas de red y de transporte, respectivamente. A diferencia de WIREGUARD, los protocolos **IPSEC y TLSv1.3 son cripto-ágiles**, lo que facilita la transición gradual hacia la criptografía post-cuántica, pues permite integrar los nuevos algoritmos PQC de manera progresiva sin necesidad de realizar cambios drásticos en la infraestructura o en las aplicaciones en uso, reduciendo el riesgo de incompatibilidades y asegurando una adopción más fluida y segura. De hecho, en ambos protocolos la hibridación se está incorporando como **extensiones opcionales**, que permiten a las partes negociar tanto el uso de las propias extensiones como de los algoritmos criptográficos y garantizar compatibilidad hacia atrás.

En el caso de **IPSEC**, existe una extensión de IKEv2, el **RFC 9370** [267], que explica cómo combinar múltiples intercambios en el cálculo de claves de sesión, tanto cuando se establece la SA principal del IKE como al crear asociaciones hijas a partir de ella. Esta extensión ya está siendo implementada en equipos de fabricantes como Palo Alto Networks [268], Cisco [269] y Fortinet [270]. Durante la fase IKE_SA_INIT, las partes negocian los intercambios adicionales que se emplearán y, para cada uno de ellos, se lleva a cabo una fase IKE_INTERMEDIATE, en la cual se actualiza la clave de sesión de forma incremental. Aunque en el RFC 9370 no se referencian algoritmos específicos, hay otras especificaciones que lo complementan instanciando algoritmos como CRYSTALS-KYBER (ML-KEM) [271] y FrodoKEM [272].

Durante la fase IKE_INTERMEDIATE correspondiente a un KEM, el emisor genera la clave pública y el receptor genera el secreto que manda encapsulado al emisor (kem_secret). Más en detalle, el emisor genera en primer lugar un par de claves $(sk, pk) = \text{Gen}()$ y envía la componente pública pk al receptor. A continuación, el receptor genera y encapsula una clave aleatoria kem_secret usando la clave pk recibida con la función $(\text{kem_secret}, c) = \text{Encap}(pk)$ y, a continuación, transmite el encapsulado c al emisor. Finalmente, el emisor puede recuperar el secreto utilizando su clave privada sk con la función $\text{kem_secret} = \text{Decap}(sk, c)$. Tras finalizar este intercambio en dos pasos, ambas partes comparten un secreto común. En la Figura 6-2 se ilustra este proceso, así como el acuerdo clásico (EC)DH para proporcionar una comparativa visual de ambas aproximaciones.

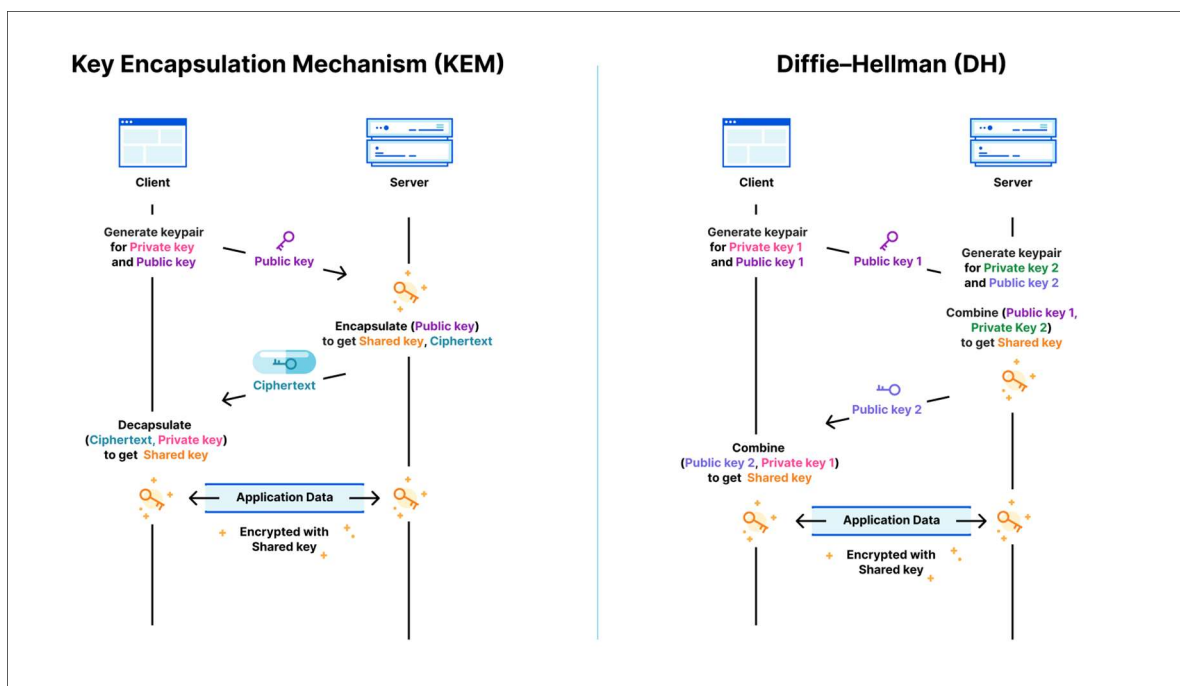


Figura 6-2 Compartición de secretos en IPSEC usando DH y KEM [273].

Si se considera el caso de IKEv2 extendido con RFC 9370, en que el acuerdo clásico es ECDH y se negocia un único intercambio adicional basado en KEM, la clave de sesión de la SA del IKE se deriva en dos pasos como sigue:

```

SKEYSEED = HMAC(nonces, ecdh_secret)
SK = {SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr} =
    PRF+(SKEYSEED, nonces | ids)
SKEYSEED* = HMAC(SK_d, kem_secret | nonces)
SK* = {SK_d* | SK_ai* | SK_ar* | SK_ei* | SK_er* | SK_pi* | SK_pr*} =
    PRF+(SKEYSEED*, nonces | ids)

```

donde las funciones PRF+ y HMAC son las definidas la sección 6.2, `ecdh_secret` es el secreto acordado en el ECDH clásico y `kem_secret` el secreto transportado por el KEM.

Por otra parte, la extensión para **TLSv1.3** se especifica en el documento **draft-ietf-tls-hybrid-design** [274], que al igual que ocurre con el RFC 9370 que extiende IPSEC, especifica cómo hacer un intercambio de claves híbrido en el AKE de TLSv1.3, pero que no referencia algoritmos KEM específicos. Existe una especificación complementaria que instancia el par de algoritmos X25519 para el ECDH clásico y CRYSTALS-KYBER-768 (ML-KEM-768) como KEM post-cuántico [275]. En este caso, el emisor propone en el CLIENT_HELLO el acuerdo clásico X25519 y el combinado X25519+ML-KEM-768 y, si el receptor implementa la extensión, lo acepta en el SERVER_HELLO y tiene lugar el establecimiento de clave de sesión híbrido entre las partes. Actores relevantes de Internet, como Google [276] y Cloudflare [277], han apostado por esta hibridación.

Los cambios que introduce draft-ietf-tls-hybrid-design en la especificación original de TLSv1.3 son mínimos. En los mensajes del AKE de tipo *key_exchange* se concatenan directamente los valores correspondientes del ECDH y del KEM que se combinan, en este orden, transmitiéndose como un valor único y evitando de esta forma modificar las estructuras o el número de mensajes que componen el AKE. Por ejemplo, en la combinación de X25519 con ML-KEM-768, el *key_exchange* del emisor concatena 32 bytes de clave pública Curve25519 con 1.184 bytes de clave pública ML-KEM-768 (1.216 en total), mientras que el *key_exchange* del receptor concatena 32 bytes de clave pública Curve25519 con 1.088 bytes de encapsulado ML-KEM-768 (1.120 en total).

En TLSv1.3 híbrido no se modifica el mecanismo de derivación de claves de sesión original del protocolo [19], basado en la función HKDF (*HMAC-based Key Derivation Function*) [278], sino que se utiliza como secreto la concatenación del secreto acordado con el ECDH y el secreto transportado con el KEM post-cuántico. Si se denomina a estos valores `ecdh_secret` y `kem_secret`, respectivamente, el secreto base para la derivación es:

```
concatenated_shared_secret = ecdh_secret | kem_secret
```

tal y como se representa en la Figura 6-3. En la combinación X25519 con ML-KEM-768, cada uno de los secretos tiene 32 bytes, por lo que el secreto concatenado son 64 bytes.

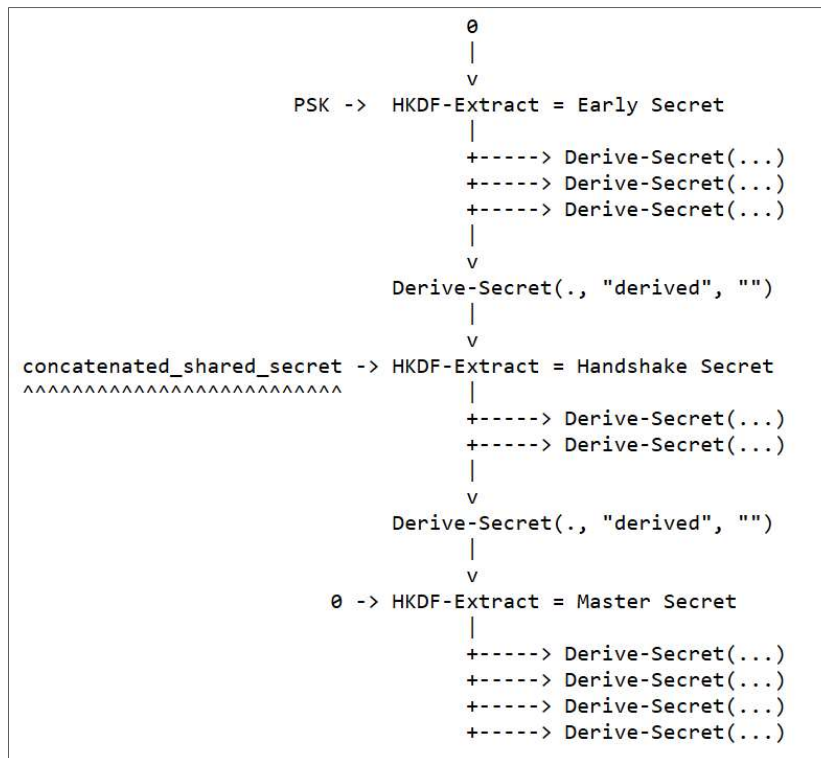


Figura 6-3 Derivación de claves de sesión en TLSv1.3 híbrido [274].

En la Figura 6-4 se representa gráficamente cómo se acuerda en TLSv1.3 híbrido el secreto compartido `concatenated_shared_secret` en el caso X22519+ML-KEM-768 [274] [275] [279]. La imagen puede parecer compleja a primera vista, como lo es el proceso que representa, pero ilustra muy bien los dos procesos criptográficos que tienen lugar en paralelo, quién es responsable de cada acción y cómo ambas partes recuperan finalmente el mismo secreto concatenado.

Primero, el emisor genera pares de claves (efímeras) tanto para X22519 como para ML-KEM-768, así como otro par de claves X22519 por si el receptor no acepta la combinación de algoritmos (en otro caso, simplemente se ignora), y manda CLIENT_HELLO con dos valores de *supported_group* y *key_exchange*, uno para el ECDH simple y otro para el combinado con el KEM. Cuando el receptor acepta el esquema combinado, genera su propio par de claves para X22519 y obtiene el secreto `ecdh_secret`. Después, genera el `kem_secret`, lo encapsula con la clave pública ML-KEM-768 del emisor y manda este encapsulado junto con su clave pública Curve25519 en el SERVER_HELLO. A partir de estos datos, el emisor desencapsula el `kem_secret` y construye el `ecdh_secret`.

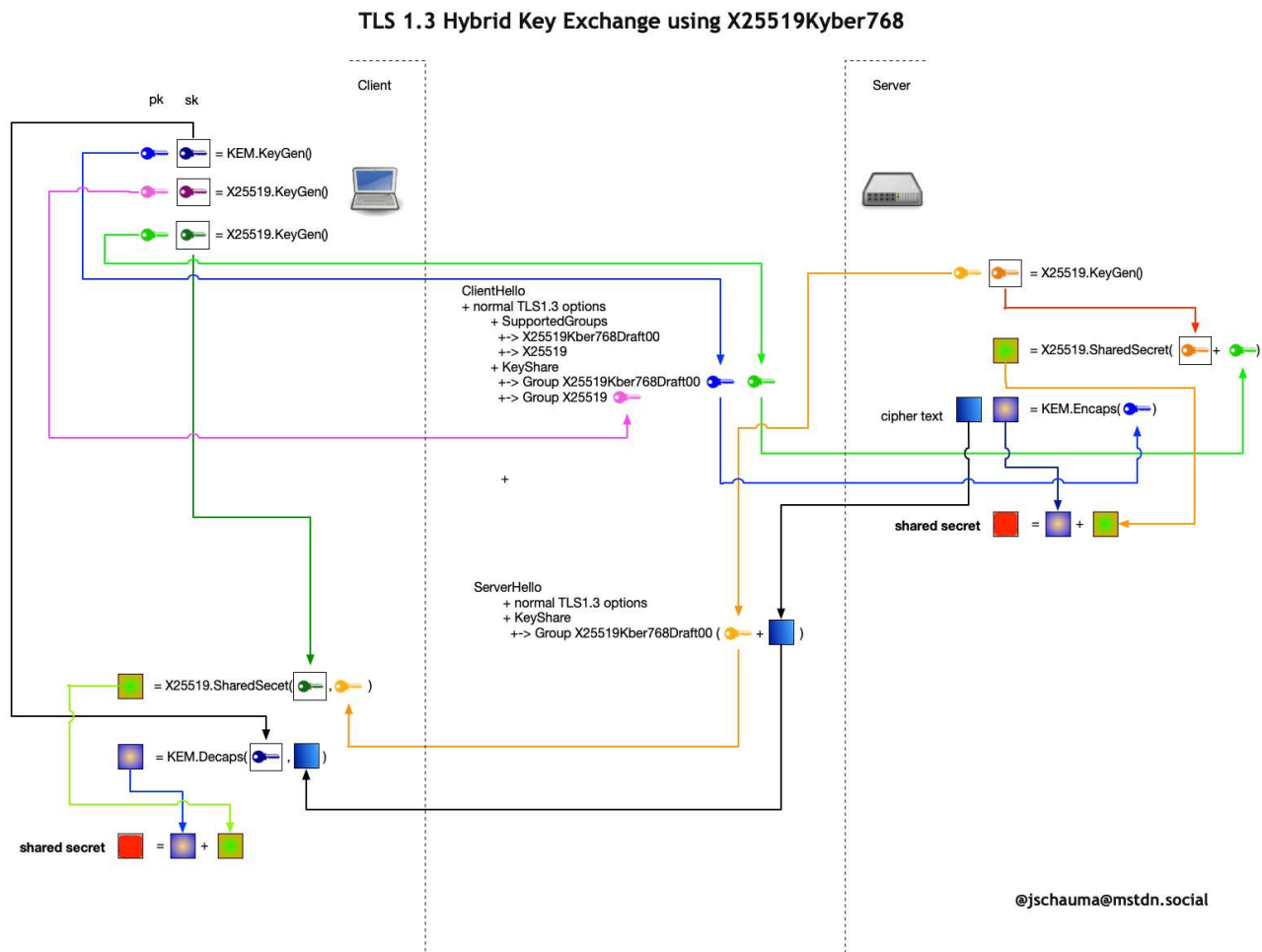


Figura 6-4 Acuerdo del secreto compartido en TLSv1.3 híbrido [279].

Desde el punto de vista de la **implementación** de protocolos criptográficos híbridos, la combinación ECDH+KEM requiere más ancho de banda y mayor tiempo de cómputo para completar el IKE que cuando se emplea solo ECDH, como se ha venido justificando a lo largo del trabajo. La penalización que supone añadir un KEM puede llegar a ser muy severa, impidiendo en la práctica que algunos algoritmos puedan utilizarse en protocolos existentes sin una revisión profunda de los mismos. En los últimos años se han publicado varios trabajos que estudian la idoneidad de algoritmos KEM para TLSv1.3, así como el impacto en sus prestaciones, a destacar [280]. Hay disponible, además, un *fork* de OpenSSL que permite probar los KEM implementados en la librería *liboqs* en TLSv1.3 [281]. Sin embargo, no se encuentran trabajos similares para IPSEC, probablemente porque no existe una implementación de código abierto como la disponible para TLSv1.3.

En [280] se comprueba que los KEM basados en retículos estructurados como CRYSTALS-KYBER, SABER o NTRU-Prime, destacan por su buen rendimiento y por el impacto moderado en el ancho banda. No es de extrañar que **CRYSTALS-KYBER**, que además ha sido ya estandarizado, sea la opción preferida para hibridación en la mayoría de los protocolos criptográficos. En el lado opuesto se encuentran Classic-McEliece, cuyo enorme tamaño de clave imposibilita directamente su uso en TLSv1.3 extendido con draft-ietf-tls-hybrid-design; también FrodoKEM y HQC que, aunque pueden integrarse en esta extensión, tienen un impacto significativo en el rendimiento, sobre todo en escenarios en los que la tasa de transmisión es baja o hay pérdida de paquetes. Un motivo del rendimiento degradado es que tamaños de clave grandes causan que los paquetes CLIENT_HELLO y SERVER_HELLO superen el MTU (*Maximum Transmission Unit*) de la red y tengan que fragmentarse.

Por último, conviene matizar que las extensiones híbridas tanto de IPSEC como de TLSv1.3 que se han presentado en esta sección permiten garantizar el **secreto hacia adelante**, pues tanto las claves de ECDH como de KEM pueden ser efímeras según las especificaciones. Sin embargo, esta propiedad depende en la práctica de la implementación concreta de los protocolos, y no se cumpliría en el caso de que emisor o receptor reutilizaran claves públicas en diferentes sesiones.

7 CONCLUSIONES

Este trabajo ha abordado la amenaza que representa el desarrollo de la computación cuántica para la seguridad de los protocolos criptográficos utilizados en las comunicaciones IP, evaluando posibles soluciones y explorando cómo integrar técnicas de resistencia cuántica en dichas comunicaciones. Se han cubierto, por tanto, los tres objetivos planteados.

Los ordenadores cuánticos tienen el potencial de comprometer la seguridad de algoritmos criptográficos utilizados en la actualidad para garantizar servicios de seguridad en Internet. Este riesgo es especialmente relevante para los algoritmos de clave pública cuya seguridad se basa en la dificultad de resolver problemas de factorización entera y logaritmo discreto en grupos finitos, ambos vulnerables al algoritmo cuántico de Shor.

La computación cuántica se encuentra aún en desarrollo, existiendo importantes retos tecnológicos que dificultan el desarrollo de un ordenador cuántico a gran escala capaz de vulnerar estos algoritmos de forma efectiva, principalmente la escalabilidad y la coherencia de los sistemas cuánticos. Aunque en los últimos años se han producido avances significativos en el desarrollo de procesadores cuánticos y de los algoritmos de corrección de errores por ruido cuántico y decoherencia, no hay un horizonte definido sobre cuándo estará disponible un ordenador cuántico criptográficamente capaz.

Las estimaciones actuales indican que es muy improbable que se construya este CRQC antes de 2030, y poco probable antes de 2035, atendiendo a las opiniones de los expertos y al ritmo de desarrollo tecnológico. Sin embargo, no se pueden descartar avances disruptivos en la escalabilidad de los procesadores cuánticos o en técnicas de corrección de errores, que puedan acelerar el desarrollo y acortar estos plazos. Además, existe el riesgo de que actores maliciosos almacenen comunicaciones cifradas para descifrarlas en el futuro con capacidades cuánticas. Estos riesgos subrayan la urgencia de avanzar hacia soluciones criptográficas resistentes a la computación cuántica, capaces de proporcionar seguridad a las comunicaciones en Internet frente a esta amenaza emergente.

Una de las alternativas es la distribución cuántica de claves (QKD). Esta tecnología permite a dos partes acordar una clave aleatoria que se comparte de forma segura a través de un canal cuántico, detectando cualquier intento de intrusión gracias a principios fundamentales de la mecánica cuántica. En la actualidad, se codifican los bits de clave en fotones transmitidos por fibra óptica o espacio libre, siendo la primera opción la más desarrollada. Aunque QKD es teóricamente segura, su implementación práctica enfrenta importantes desafíos, como ataques de denegación de servicio y vulnerabilidades en los dispositivos opto-electrónicos empleados. Además, esta tecnología tiene limitaciones significativas en cuanto al alcance de las comunicaciones por la atenuación de la señal fotónica y la baja tasa de generación de claves derivada de los mecanismos utilizados para generar e interpretar dicha señal.

Aunque se están investigando tecnologías que permitan extender el alcance de QKD manteniendo sus propiedades de seguridad cuántica, como los repetidores cuánticos y las memorias cuánticas, estas soluciones aún no han alcanzado la madurez necesaria. Por este motivo, las redes actuales de QKD dependen de repetidores clásicos para la retransmisión de claves, una solución que compromete la seguridad incondicional teórica de la QKD, pues los nodos intermedios deben recuperar y gestionar las claves, exigiendo la confianza de los comunicantes. Además, el elevado coste de las infraestructuras dedicadas requeridas, la falta de estándares que garanticen la interoperabilidad entre distintos sistemas y la necesidad de canales auxiliares para la autenticación siguen representando barreras significativas para su adopción como una solución universal. Sin embargo, proyectos experimentales están explorando infraestructuras de comunicación cuántica, tanto terrestres como satelitales, con el objetivo a largo plazo de construir un Internet cuántico que proporcione seguridad a escala global.

La criptografía post-cuántica (PQC) también proporciona resistencia cuántica. Los algoritmos de clave pública de PQC evitan las bases matemáticas vulnerables utilizadas por los algoritmos clásicos y emplean en su lugar problemas alternativos como retículos, códigos de corrección de errores e isogenias de curvas elípticas, entre otros. Estos fundamentos matemáticos alternativos proporcionan robustez teórica frente a ataques tanto clásicos como cuánticos, evitando invertir en infraestructura dedicada como las que necesitan las comunicaciones cuánticas. Los algoritmos post-cuánticos de encapsulamiento de claves y firma digital han sido objeto de un extenso proceso de evaluación y estandarización en los últimos años, que ha culminado recientemente con la aprobación de los primeros estándares de encapsulamiento (ML-KEM) y firma (ML-DSA, SLH-DSA) por el NIST. Además, se siguen evaluando algoritmos de encapsulamiento basados en códigos como alternativa a ML-KEM, basado en retículos, y el NIST está estandarizando otro algoritmo de retículos que genera firmas más cortas que ML-DSA.

A pesar de constituir una alternativa más simple y accesible que QKD, por su compatibilidad con las infraestructuras existentes, los algoritmos post-cuánticos también presentan desafíos. En términos prácticos, suelen requerir claves, firmas y cifrados de mayor tamaño que los algoritmos clásicos, lo que implica un aumento del coste computacional y posibles limitaciones de rendimiento. Desde el punto de vista de la seguridad, su mayor complejidad matemática dificulta garantizar la ausencia de vulnerabilidades, tanto teóricas como de implementación. Esto ha llevado a que varios esquemas prometedores hayan sido vulnerados incluso en fases avanzadas del proceso de estandarización del NIST, como esquemas finalistas basados en isogenias y polinomios multivariantes que se postulaban como alternativas a ML-KEM y ML-DSA para seguridad en comunicaciones.

Independientemente de la solución que se elija para dotar de resistencia cuántica a los protocolos criptográficos de comunicaciones IP, el enfoque principal debe dirigirse a los mecanismos de autenticación y establecimiento de claves de sesión, ya que el uso de criptografía simétrica con longitudes de clave suficientes sigue proporcionando un nivel adecuado de seguridad para la transmisión de datos cifrados y autenticados. Sin embargo, el establecimiento de claves representa actualmente el mayor punto de vulnerabilidad, ya que potenciales adversarios podrían almacenar comunicaciones cifradas actuales para descifrarlas en el futuro con ordenadores cuánticos. Por esta razón, las primeras fases de la transición hacia soluciones resistentes a la computación cuántica están priorizando este aspecto crítico, relegando a un segundo plano la actualización de los mecanismos de autenticación en los protocolos de Internet.

El empleo de claves simétricas pre-compartidas constituye la solución más sencilla para dotar de resistencia cuántica a las comunicaciones sin necesidad de modificar infraestructuras ni algoritmos existentes, aunque también es la menos escalable y no permite el secreto hacia adelante ante un adversario con capacidades cuánticas. Por otra parte, QKD es una solución atractiva por la excelente seguridad teórica que ofrece, pero su adopción generalizada se ve limitada por el nivel de madurez de la tecnología y la necesidad de equipamiento costoso e infraestructura dedicada. Esto la posiciona como una posible solución a medio plazo para redes con pocos usuarios y de cobertura limitada, donde los requisitos de seguridad justifiquen la elevada inversión que implica. En contraste, PQC se perfila como la alternativa más práctica, flexible y viable para su integración en los principales protocolos actuales de Internet, como IPSEC o TLS.

La estrategia más recomendable para la transición hacia protocolos resistentes a la computación cuántica es emplear enfoques híbridos, que combinen algoritmos clásicos y post-cuánticos, reduciendo así los riesgos asociados a la sustitución inmediata de algoritmos maduros por otros más recientes que todavía están bajo el escrutinio de la comunidad científica. Una característica útil de los protocolos para garantizar el éxito de esta transición es la cripto-agilidad, que permite cambiar algoritmos de manera flexible a medida que evolucionan las amenazas o se identifican vulnerabilidades. Por ahora, la hibridación es la solución más conservadora, aunque en el futuro los protocolos podrían depender exclusivamente de algoritmos post-cuánticos. Las soluciones híbridas que se están implementando en protocolos como IPSEC, TLS, SSH y SIGNAL permiten una transición progresiva, además de asegurar la interoperabilidad con las infraestructuras actuales, sentando las bases para un futuro más seguro en las comunicaciones IP.

8 BIBLIOGRAFÍA

En esta sección se listan las referencias citadas a lo largo del trabajo, en el orden en que se referencian y citadas siguiendo el estilo IEEE.

- [1] A. J. Menezes, J. Katz, P. C. van Oorschot y S. A. Vanstone, “Handbook of applied cryptography”, CRC Press, 2018.
- [2] D. Boneh y V. Shoup, “A graduate course in applied cryptography”, Cryptobook.us. [En línea]. Disponible en: <https://toc.cryptobook.us/book.pdf> [Consultado: 05-nov-2024].
- [3] C. Boyd, A. Mathuria y D. Stebila, “Protocols for authentication and key establishment”, 2ª ed, Springer, 2019.
- [4] B. Kacsmar y T. Humphries, “CS 489 / 689 - privacy, cryptography, network and data security - winter 2023”, Universidad de Waterloo. [En línea]. Disponible en: <https://crysp.uwaterloo.ca/courses/data-sp/W23/index.html>. [Consultado: 02-ene-2025].
- [5] B. Kacsmar y T. Humphries, “CS 489 / 689 - privacy, cryptography, network and data security - winter 2023. Lecture 11 slides”, Universidad de Waterloo. [En línea]. Disponible en: https://crysp.uwaterloo.ca/courses/data-sp/W23/slides/lecture_11.pdf. [Consultado: 02-ene-2025].
- [6] “802.1AE-2006: IEEE standard for local and metropolitan area networks: Media access control (MAC) security”, IEEE, Piscataway, NJ, USA, 2006.
- [7] “802.11-2020: IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements”, IEEE, Piscataway, NJ, USA, 2004.
- [8] “802.11ax-2021: IEEE standard for information technology - Telecommunications and information exchange between systems local and metropolitan area networks - Specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 1: Enhancements for high-efficiency WLAN”, IEEE, Piscataway, NJ, USA, 2021.
- [9] S. Karr, “Core specification 6.0”, Bluetooth Technology Website, sep-2024. [En línea]. Disponible en: <https://www.bluetooth.com/specifications/specs/core60-html>. [Consultado: 30-dic-2024].
- [10] “802.15.4-2015: IEEE Standard for Low-Rate Wireless Networks”, IEEE, Piscataway, NJ, USA, 2016.
- [11] “Reference manual for OpenVPN 2.4”, OpenVPN. [En línea]. Disponible en: <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4>. [Consultado: 02-ene-2025].
- [12] J. A. Donenfeld, “WireGuard: Next Generation Kernel Network Tunnel”, en Proceedings 2017 Network and Distributed System Security Symposium, 2017.
- [13] D. Harkins y D. Carrel, “The Internet Key Exchange (IKE)”, RFC 2409, nov-1998. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc2409>. [Consultado: 02-ene-2025].
- [14] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen y T. Kivinen, “Internet Key Exchange Protocol Version 2 (IKEv2)”, RFC 7296, oct-2014. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc7296>. [Consultado: 02-ene-2025].
- [15] S. Kent, “IP Encapsulating Security Payload (ESP)”, RFC 4303, dic-2005. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc4303>. [Consultado: 02-ene-2025].
- [16] E. Rescorla y N. Modadugu, “Datagram Transport Layer Security version 1.2”, RFC 6347, ene-2012. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc6347>. [Consultado: 02-ene-2025].
- [17] J. Iyengar y M. Thomson, “QUIC: A UDP-based multiplexed and secure transport”, RFC 9000, may-2021. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc9000>. [Consultado: 02-ene-2025].
- [18] T. Dierks y E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, ago-2008. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc5246>. [Consultado: 02-ene-2025].

- [19] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, ago-2018. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc8446>. [Consultado: 02-ene-2025].
- [20] T. Ylonen y C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, ene-2006. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc4251>. [Consultado: 31-dic-2024].
- [21] J. Schaad, B. Ramsdell y S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, abr-2019. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc8551>. [Consultado: 31-dic-2024].
- [22] J. Callas, L. Donnerhake, H. Finney, D. Shaw y R. Thayer, "OpenPGP Message Format", RFC 4880, nov-2007. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc4880>. [Consultado: 02-ene-2025].
- [23] "GnuPG - The GNU Privacy Guard", GNU Privacy Guard [En línea]. Disponible en: <https://gnupg.org>. [Consultado: 31-dic-2024].
- [24] K. Cohn-Gordon, C. J. F. Cremers, B. Dowling, L. Garratt, y D. Stebila, "A formal security analysis of the signal messaging protocol", Journal of Cryptology, vol. 33, pp. 1914–1983, 2017.
- [25] D. Kahn, "The Codebreakers", Macmillan, 1974.
- [26] NIST, "Data Encryption Standard (DES)", FIPS PUB 46, 1977.
- [27] W. Diffie y M. E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, vol. 22, núm. 6, pp. 644-654, 1976.
- [28] R. L. Rivest, A. Shamir y L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, núm. 2, pp. 120-126, 1978.
- [29] Medium.com. [En línea]. Disponible en: https://miro.medium.com/v2/resize:fit:960/1*8bpa0SfEU3TOe7D2FGxXDA.png. [Consultado: 28-dic-2024].
- [30] Researchgate.net. [En línea]. Disponible en: <https://www.researchgate.net/profile/Amine-Khalidi/publication/325206752/figure/fig6/AS:627405483937794@1526596532232/The-Diffie-Hellman-key-exchange.png>. [Consultado: 30-dic-2024].
- [31] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. Inf. Theory, vol. 31, núm. 4, pp. 469–472, 1985.
- [32] ISO, "Information technology - Security techniques - Digital signatures - Mechanisms based on the RSA algorithm", ISO/IEC 9796, 1991.
- [33] NIST, "Digital Signature Standard (DSS)", FIPS PUB 186, 1994.
- [34] Vietnix.vn. [En línea]. Disponible en: <https://vietnix.vn/wp-content/uploads/2021/06/digital-signatures.jpg>. [Consultado: 29-dic-2024].
- [35] NIST, "Advanced Encryption Standard (AES)", FIPS PUB 197, 2001.
- [36] Nist.gov. [En línea]. Disponible en: <https://www.nist.gov/news-events/news/2000/10/commerce-department-announces-winner-global-information-security>. [Consultado: 29-dic-2024].
- [37] Nist.gov. [En línea]. Disponible en: <https://www.nist.gov/news-events/news/1999/08/nist-announces-encryption-standard-finalists>. [Consultado: 29-dic-2024].
- [38] ISO, "Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers", ISO/IEC 18033-3, 2010.
- [39] Y. Nir y A. Langley, "ChaCha20 and Poly1305 for IETF Protocols", IRTF Request For Comments 8439, 2018.
- [40] C. Dobraunig, M. Eichlseder, F. Mendel, y M. Schläffer, "Ascon v1.2: Lightweight authenticated encryption and hashing", Journal of Cryptology, vol. 34, núm. 3, 2021.

- [41] Nist.gov. [En línea]. Disponible en: <https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices>. [Consultado: 29-dic-2024].
- [42] V. S. Miller, "Use of elliptic curves in cryptography", *Advances in Cryptology - CRYPTO '85*, vol. 218, pp. 417-426, 1986.
- [43] NIST, "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography", NIST SP 800-56A Rev. 3, 2018.
- [44] NIST, "Digital Signature Standard (DSS)", FIPS PUB 186-5, 2023.
- [45] S. Josefsson, I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, ene-2017. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc8032>. [Consultado: 30-dic-2024].
- [46] C. E. Shannon, "A mathematical theory of communication", *Bell Syst. Tech. J.*, vol. 27, núm. 3, pp. 379-423, 1948.
- [47] J. Chia, J.-J. Chin, y S.-C. Yip, "Digital signature schemes with strong existential unforgeability", *F1000Res.*, vol. 10, p. 931, 2021.
- [48] B. C. Neuman y T. Ts'o, "Kerberos: an authentication service for computer networks", *IEEE Commun. Mag.*, vol. 32, núm. 9, pp. 33-38, 1994.
- [49] H. Haverinen y J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, ene-2006. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc4186>. [Consultado: 30-dic-2024].
- [50] J. Arkko, V. Lehtovirta, V. Torvinen, y P. Eronen, "Improved Extensible Authentication Protocol method for 3GPP mobile network authentication and Key Agreement (EAP-AKA')", RFC 9048, oct-2021. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc9048>. [Consultado: 30-dic-2024].
- [51] R. Housley, W. Polk, W. Ford y D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, may-2008. [En línea]. Disponible en: <https://datatracker.ietf.org/doc/rfc5280>. [Consultado: 23-nov-2024].
- [52] M. Myers, R. Ankney, A. Malpani, S. Galperin y C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", RFC 2560, jun-1999. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc2560>. [Consultado: 30-dic-2024].
- [53] A. Ulrich, R. Holz, P. Hauck, y G. Carle, "Investigating the OpenPGP web of trust", en *Computer Security - ESORICS 2011*, Springer Berlin Heidelberg, pp. 489-507, 2011.
- [54] T. Perrin, "The Noise protocol framework", [Noiseprotocol.org](https://noiseprotocol.org/noise.pdf). [En línea]. Disponible en: <https://noiseprotocol.org/noise.pdf>. [Consultado: 31-dic-2024].
- [55] NIST, "The Keyed-Hash Message Authentication Code (HMAC)", FIPS PUB 198-1, 2008.
- [56] NIST, "SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash", NIST SP 800-185, 2016.
- [57] NIST, "Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication", NIST SP 800-38B, 2016.
- [58] M. Bellare y C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm", en *Advances in Cryptology ASIACRYPT 2000*, Springer Berlin Heidelberg, pp. 531-545, 2000.
- [59] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)", en *Advances in Cryptology CRYPTO 2001*, Springer Berlin Heidelberg, pp. 310-331, 2001.
- [60] M. Bellare, T. Kohno, y C. Namprempre, "Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm", *ACM Trans. Inf. Syst. Secur.*, vol. 7, núm. 2, pp. 206-241, 2004.

- [61] NIST, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”, NIST SP 800-38D, 2007.
- [62] E. Ozturk, T. Kantecki y K. Yap, “Advanced Encryption Standard Galois Counter Mode - Optimized GHASH Function”, Intel.com. [En línea]. Disponible en: <https://networkbuilders.intel.com/docs/networkbuilders/advanced-encryption-standard-galois-counter-mode-optimized-ghash-function-technology-guide-1693300747.pdf>. [Consultado: 9-nov-2024].
- [63] J. Black, “Authenticated encryption”, en *Encyclopedia of Cryptography and Security*, Springer US, pp. 11–21, 2006.
- [64] NIST, “Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality”, NIST SP 800-38C, 2007.
- [65] NIST, "Post-Quantum Cryptography Standardization: Call for Proposals", NIST Computer Security Resource Center, 3-ene-2017. [En línea]. Disponible en: <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals>. [Consultado: 7-sept-2024].
- [66] M. Mosca y M. Piani, “2023 quantum threat timeline report”, Global Risk Institute, 22-dic-2023. [En línea]. Disponible en: <https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report>. [Consultado: 7-sep-2024].
- [67] J. Schneider y I. Smalley, "Quantum Computing", Ibm.com, 30-ago-2024. [En línea]. Disponible en: <https://www.ibm.com/es-es/topics/quantum-computing>. [Consultado: 14-Sep-2024].
- [68] J. Schneider y I. Smalley, "What is a qubit?", Ibm.com, 23-ago-2024. [En línea]. Disponible en: <https://www.ibm.com/topics/qubit>. [Consultado: 14-sep-2024].
- [69] J. Fingas, “IBM quantum computers now finish some tasks in hours, not months”, Engadget, 04-feb-2021. [En línea]. Disponible en: <https://www.engadget.com/ibm-quantum-computing-speedup-050134678.html>. [Consultado: 7-sep-2024].
- [70] A. Techlady, “Qubit”, Devopedia, 05-ene-2022. [En línea]. Disponible en: <https://devopedia.org/qubit>. [Consultado: 14-sep-2024].
- [71] R. Feynman, "Simulating Physics with Computers", *International Journal of Theoretical Physics*, vol. 21, núm. 6–7, pp. 467–488, 1982.
- [72] P. Benioff, “The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Interacting Quantum Mechanical Spins”, *Journal of Statistical Physics*, vol. 22, núm. 5, pp. 563–591, 1980.
- [73] D. Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," *Proceedings of the Royal Society of London. A, Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97-117, 1985.
- [74] M. Mosca, “Quantum Algorithms”, arXiv [quant-ph], 2008.
- [75] N. A. Gershenfeld y I. L. Chuang, “Bulk spin-resonance quantum computation”, *Science*, vol. 275, núm. 5298, pp. 350–356, 1997.
- [76] L. M. K. Vandersypen et al., "Implementation of the Shor Quantum Factoring Algorithm Using a Superconducting Qubit Quantum Processor," *Nature*, vol. 419, pp. 23-26, 2001.
- [77] H. Liu, G. H. Low, D. S. Steiger, T. Häner, M. Reiher, y M. Troyer, “Prospects of quantum computing for molecular sciences”, *Materials Theory*, vol. 6, núm. 1, 2022.
- [78] K. Zaman, A. Marchisio, M. A. Hanif, y M. Shafique, “A survey on Quantum Machine Learning: Current trends, challenges, opportunities, and the road ahead”, arXiv [quant-ph], 2023.
- [79] S. P. Jordan y Y.-K. Liu, "Quantum Cryptanalysis: Shor, Grover, and Beyond", *IEEE Security & Privacy*, vol. 16, núm. 5, pp. 14-21, 2018.

- [80] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", Proceedings of the 35th Annual ACM Symposium on Theory of Computing, pp. 124-134, 1994.
- [81] J. P. Buhler, H. W. Lenstra Jr, y C. Pomerance, "Factoring integers with the number field sieve", en Lecture Notes in Mathematics, Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 50-94.
- [82] R. P. Brent, "Improved upper bound for the General Number Field Sieve algorithm," Mathematics of Computation, vol. 70, no. 236, pp. 747-759, 2000.
- [83] F. Boudot, P. Gaudry, A. Guillevis, N. Heninger, E. Thomé, y P. Zimmermann, "Factoring RSA-250 with PRACE", Loria.fr. [En línea]. Disponible en: <https://members.loria.fr/PZimmermann/talks/rsa250-prace.pdf>. [Consultado: 18-sep-2024].
- [84] M. Ekerå, "On completely factoring any integer efficiently in a single run of an order-finding algorithm", Quantum Inf. Process., vol. 20, núm. 6, 2021.
- [85] C.-Y. Lu, D. E. Browne, T. Yang, y J.-W. Pan, "Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits", Physical Review Letters, vol. 99, núm. 25, p. 250504, 2007.
- [86] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland y J. M. Martinis, "Computing prime factors with a Josephson phase qubit quantum processor", Nature Physics, vol. 8, núm. 10, pp. 719-723, 2012.
- [87] E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, y J. L. O'Brien, "Experimental realisation of Shor's quantum factoring algorithm using qubit recycling", Conference on Lasers & Electro-Optics Europe & International Quantum Electronics Conference CLEO EUROPE/IQEC, 2013.
- [88] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, y R. Blatt, "Realization of a scalable Shor algorithm", Science, vol. 351, núm. 6277, pp. 1068-1070, 2016.
- [89] M. Amico, Z. H. Saleem, y M. Kumph, "Experimental study of Shor's factoring algorithm using the IBM Q Experience", arXiv [quant-ph], 2019.
- [90] L. K. Grover, "A fast quantum mechanical algorithm for database search", Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996.
- [91] C. H. Bennett, E. Bernstein, G. Brassard y U. Vazirani, "The strengths and weaknesses of quantum computation", SIAM Journal on Computing, vol. 26, núm. 5, pp. 1510-1523, 1997.
- [92] K.-A. Brickman, P. C. Haljan, P. J. Lee, M. Acton, L. Deslauriers, y C. Monroe, "Implementation of Grover's quantum search algorithm in a scalable system", Physical Review A, vol. 72, núm. 5, 2005.
- [93] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, y C. Monroe, "Complete 3-qubit Grover search on a programmable quantum computer", arXiv [quant-ph], 2017.
- [94] A. Mandviwalla, K. Ohshiro, y B. Ji, "Implementing Grover's algorithm on the IBM quantum computers", en 2018 IEEE International Conference on Big Data (Big Data), 2018.
- [95] K. Zhang, P. Rao, K. Yu, H. Lim, y V. Korepin, "Implementation of efficient quantum search algorithms on NISQ computers", Quantum Inf. Process., vol. 20, núm. 7, 2021.
- [96] K. Zhang, K. Yu, y V. Korepin, "Quantum search on noisy intermediate-scale quantum devices", EPL, vol. 140, núm. 1, p. 18002, 2022.
- [97] B. Pokharel y D. A. Lidar, "Better-than-classical Grover search via quantum error detection and suppression", Npj Quantum Inf., vol. 10, núm. 1, 2024.
- [98] J. Roffe, "Quantum error correction: an introductory guide", Contemporary Physics, vol. 60, núm. 3, pp. 226-245, 2019.
- [99] Google Quantum AI, "Our focused and responsible approach to quantum computing," Google Inc., 2021. [En línea]. Disponible en: <https://quantumai.google>. [Accedido: 18-Sep-2024].
- [100] F. Arute et al., "Quantum supremacy using a programmable superconducting processor", Nature, vol. 574, núm. 7779, pp. 505-510, 2019.

- [101] Google Quantum AI, “Suppressing quantum errors by scaling a surface code logical qubit”, *Nature*, vol. 614, núm. 7949, pp. 676–681, 2023.
- [102] H. Neven, “Meet Willow, our state-of-the-art quantum chip”, Google, 09-dic-2024. [En línea]. Disponible en: <https://blog.google/technology/research/google-willow-quantum-chip>. [Consultado: 13-dic-2024].
- [103] R. Acharya et al., “Quantum error correction below the surface code threshold”, *arXiv [quant-ph]*, 2024.
- [104] “IBM Quantum roadmap to build quantum-centric supercomputers”, *Ibm.com*. [En línea]. Disponible en: <https://www.ibm.com/quantum/blog/ibm-quantum-roadmap-2025>. [Consultado: 21-sep-2024].
- [105] “IBM Quantum System Two: the era of quantum utility is here”, *Ibm.com*. [En línea]. Disponible en: <https://www.ibm.com/quantum/blog/quantum-roadmap-2033>. [Consultado: 21-sep-2024].
- [106] “IBM Quantum delivers on 2022 100x100 performance challenge”, *Ibm.com*. [En línea]. Disponible en: <https://www.ibm.com/quantum/blog/qdc-2024>. [Consultado: 13-dic-2024].
- [107] Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing, Computer Science and Telecommunications Board, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, y National Academies of Sciences, Engineering, and Medicine, “Quantum Computing: Progress and Prospects”. National Academies Press, Washington, D.C., 2019.
- [108] A. G. Fowler, M. Mariantoni, J. M. Martinis, y A. N. Cleland, “Surface codes: Towards practical large-scale quantum computation”, *Phys. Rev. A*, vol. 86, núm. 3, 2012.
- [109] C. Gidney y M. Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”, *Quantum*, vol. 5, núm. 433, p. 433, 2021.
- [110] C. Chevalignard, P. A. Fouque y A. Schrottenloher, “Reducing the Number of Qubits in Quantum Factoring,” *Cryptology ePrint Archive*, Paper 2024/222, 2024.
- [111] J.-Y. Cai, “Shor’s algorithm does not factor large integers in the presence of noise”, *Sci. China Inf. Sci.*, vol. 67, núm. 7, 2024.
- [112] M. Mosca, “Cybersecurity in an era with quantum computers: Will we be ready?”, *IEEE Security and Privacy*, vol. 16, núm. 5, pp. 38–41, 2018.
- [113] G. Brassard, “Brief history of quantum cryptography: a personal perspective”, *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, 2005.
- [114] C. H. Bennett y G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, *Proceedings of IEEE International Conference on Computers, Systems & Signal Processing*, Bangalore, India, pp. 175 – 179, 1984.
- [115] A. Broadbent y C. Schaffner, “Quantum cryptography beyond quantum key distribution”, *arXiv [quant-ph]*, 2015.
- [116] H. J. Kimble, “The Quantum Internet”, *arXiv [quant-ph]*, 2008.
- [117] A. Abelem, D. Towsley y G. Vardoyan, “Quantum Internet: The Future of Internetworking”, *arXiv [cs.NI]*, 2023.
- [118] D. J. Bernstein, J. Buchmann y E. Dahmen (editores), “Post-Quantum Cryptography”, Springer, 2009.
- [119] NIST, “Post-quantum cryptography FIPS approved”, NIST Computer Security Resource Center, 13-ago-2024. [En línea]. Disponible en: <https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved>. [Consultado: 05-oct-2024].
- [120] ETSI, “Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges”, *European Telecommunications Standards Institute White Paper* núm. 8, 2015.
- [121] V. Mannalath, S. Mishra, y A. Pathak, “A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness”, *arXiv [quant-ph]*, 2022.

- [122] M. Sabani, I. Savvas, D. Poulakis, y G. Makris, “Quantum key distribution: Basic protocols and threats”, en Proceedings of the 26th Pan-Hellenic Conference on Informatics, 2022.
- [123] D. P. Nadlinger et al., “Experimental quantum key distribution certified by Bell’s theorem”, arXiv [quant-ph], 2021.
- [124] C.-W. Tsai, C.-W. Yang, J. Lin, Y.-C. Chang, y R.-S. Chang, “Quantum key distribution networks: Challenges and future research issues in security”, Applied Sciences (Basel), vol. 11, núm. 9, p. 3767, 2021.
- [125] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, y M. Peev, “The security of practical quantum key distribution”, arXiv [quant-ph], 2008.
- [126] “Products”, ID Quantique. [En línea]. Disponible en: <https://www.idquantique.com/quantum-safe-security/products>. [Consultado: 26-oct-2024].
- [127] “MagiQ QPNTM”, MagiQ Technologies, 12-sep-2018. [En línea]. Disponible en: <https://www.magiqtech.com/solutions/network-security>. [Consultado: 26-oct-2024].
- [128] “MAN QKD products QuantumCTek– quantum secures every bit”, Quantum-info.com. [En línea]. Disponible en: <http://quantum-info.com/English/product>. [Consultado: 26-oct-2024].
- [129] “Quantum key distribution - what is QKD? How does it work?”, Toshiba Quantum Technology, 12-sep-2024. [En línea]. Disponible en: <https://www.toshiba.eu/quantum/products/quantum-key-distribution>. [Consultado: 26-oct-2024].
- [130] Y. Zhang, Y. Bian, Z. Li, S. Yu, y H. Guo, “Continuous-variable quantum key distribution system: Past, present, and future”, Appl. Phys. Rev., vol. 11, núm. 1, 2024.
- [131] “Quantum cryptography solutions - LuxQuanta”, Luxquanta.com. [En línea]. Disponible en: <https://www.luxquanta.com/solutions>. [Consultado: 26-oct-2024].
- [132] U. J. J. Bertelsen, “100 kilometres of quantum-encrypted transfer”, Dtu.dk. [En línea]. Disponible en: <https://www.dtu.dk/english/newsarchive/2024/04/100-kilometres-of-quantum-encrypted-transfer>. [Consultado: 26-oct-2024].
- [133] V. Scarani, A. Acín, G. Ribordy, y N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations”, Phys. Rev. Lett., vol. 92, núm. 5, 2004.
- [134] D. Bruss, “Optimal eavesdropping in quantum cryptography with six states”, Phys. Rev. Lett., vol. 81, núm. 14, pp. 3018–3021, 1998.
- [135] A. Carrasco-Casado, V. Fernández y N. Denisenko, “Free-space quantum key distribution”, arXiv [physics.optics], 2016.
- [136] C. H. Bennett, G. Brassard, C. Crepeau y U. M. Maurer, “Generalized privacy amplification”, en IEEE Transactions on Information Theory, vol. 41, núm. 6, pp. 1915-1923, 1995.
- [137] A. K. Ekert, “Quantum cryptography based on Bell’s theorem”, Physical Review Letters, vol. 67, núm. 6, pp. 661–663, 1991.
- [138] C. H. Bennett, G. Brassard, y N. D. Mermin, “Quantum cryptography without Bell’s theorem”, Physical Review Letters, vol. 68, núm. 5, pp. 557–559, 1992.
- [139] K. Inoue, E. Waks, y Y. Yamamoto, “Differential phase shift quantum key distribution”, Phys. Rev. Lett., vol. 89, núm. 3, p. 037902, 2002.
- [140] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, y H. Zbinden, “Coherent one-way quantum key distribution”, en Photon Counting Applications, Quantum Optics, and Quantum Cryptography, 2007.
- [141] F. G. Paauw, A. Fedorov, C. J. P. M. Harmans, y J. E. Mooij, “Tuning the gap of a superconducting flux qubit”, Phys. Rev. Lett., vol. 102, núm. 9, p. 090501, 2009.
- [142] M. Lucamarini et al., “Efficient decoy-state quantum key distribution with quantified security”, Opt. Express, vol. 21, núm. 21, pp. 24550–24565, 2013.

- [143] D. Halevi et al., “High-dimensional quantum key distribution using orbital angular momentum of single photons from a colloidal quantum dot at room temperature”, arXiv [quant-ph], 2024.
- [144] C.-Y. Lu, Y. Cao, C.-Z. Peng, y J.-W. Pan, “Micius quantum experiments in space”, *Rev. Mod. Phys.*, vol. 94, núm. 3, 2022.
- [145] C. Pacher et al., “Attacks on quantum key distribution protocols that employ non-ITS authentication”, arXiv [quant-ph], 2012.
- [146] H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances”, *Science* 283, 2050 (1999).
- [147] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol”, *Phys. Rev. Lett.* 85, 441 (2000).
- [148] M. Koashi, “Simple security proof of quantum key distribution based on complementarity”, *New J. Phys.* 11, 045018 (2009).
- [149] ETSI, “Implementation Security of Quantum Cryptography. Introduction, challenges, solutions”, European Telecommunications Standards Institute White Paper núm. 27, 2018.
- [150] G. Brassard, N. Lutkenhaus, T. Mor y B. C. Sanders, “Limitations on practical quantum cryptography”, *Phys. Rev. Lett.*, vol. 85, núm. 6, pp. 1330–1333, 2000.
- [151] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen y H.-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems”, *Phys. Rev. A*, vol. 78, núm. 4, 2008.
- [152] B. Qi, C.-H. F. Fung, H.-K. Lo y X. Ma, “Time-shift attack in practical quantum cryptosystems”, arXiv [quant-ph], 2005.
- [153] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt y G. Leuchs, “Trojan-horse attacks threaten the security of practical quantum cryptography”, arXiv [quant-ph], 2014.
- [154] L. Lydersen et al., “Hacking commercial quantum cryptography systems by tailored bright illumination”, *Nature Photon* 4, pp. 686–689, 2010.
- [155] A. Huang et al., “Laser seeding attack in quantum key distribution”, arXiv [quant-ph], 2019.
- [156] H.-K. Lo, X. Ma, y K. Chen, “Decoy state quantum key distribution”, *Phys. Rev. Lett.*, vol. 94, núm. 23, pp. 230-504, 2005.
- [157] E. Dervisevic et al., “Simulations of denial of service attacks in quantum key distribution networks”, XXVIII International Conference on Information, Communication and Automation Technologies, 2022.
- [158] A. M. Lewis y P. F. Scudo, “Quantum communications infrastructure architecture: theoretical background, network structure and technologies. A review of recent studies from a European public infrastructure perspective”, arXiv [quant-ph], 2021.
- [159] A. Sebastián-Lombrana et al., “A blueprint for large-scale quantum-network deployments”, arXiv [quant-ph], 2024.
- [160] K. Azuma et al., “Quantum repeaters: From quantum networks to the quantum Internet”, arXiv [quant-ph], 2022.
- [161] “Madrid Quantum – Desbloqueando el Poder de las Comunicaciones Cuánticas para un Mundo más Seguro”, Madqci.es. [En línea]. Disponible en: <https://madqci.es>. [Consultado: 27-oct-2024].
- [162] “The European quantum communication infrastructure (EuroQCI) initiative”, Shaping Europe’s digital future. [En línea]. Disponible en: <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>. [Consultado: 27-oct-2024].
- [163] V. Martin et al., “MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities”, *Npj Quantum Inf.*, vol. 10, núm. 1, 2024.

- [164] S.-K. Liao et al., “Satellite-to-ground quantum key distribution”, *Nature*, vol. 549, núm. 7670, pp. 43–47, 2017.
- [165] O. Lee y T. Vergoossen, “An updated analysis of satellite quantum-key distribution missions”, *arXiv [quant-ph]*, 2019.
- [166] D. Orsucci et al., “Assessment of practical satellite quantum key distribution architectures for current and near-future missions”, *arXiv [quant-ph]*, 2024.
- [167] A. Khmelev et al., “Eurasian-scale experimental satellite-based quantum key distribution with detector efficiency mismatch analysis”, *Opt. Express*, vol. 32, núm. 7, pp. 11964–11978, 2024.
- [168] “Caramuel”, *Esa.int*. [En línea]. Disponible en: <https://connectivity.esa.int/projects/caramuel>. [Consultado: 05-nov-2024].
- [169] P. James, S. Laschet, S. Ramacher, y L. Torresetti, “Key management systems for large-scale quantum key distribution networks”, en *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023.
- [170] E. Dervisevic et al., “Quantum Key Distribution networks -- key management: A survey”, *arXiv [cs.CR]*, 2024.
- [171] O. Alia, A. Huang, H. Luo, O. Amer, M. Pistoia, y C. Lim, “100 Gbps Quantum-safe IPsec VPN Tunnels over 46 km Deployed Fiber”, *arXiv [quant-ph]*, 2024.
- [172] ETSI, “Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API”, ETSI GS QKD 014, V1.1.1, 2019.
- [173] ETSI, “Quantum Key Distribution (QKD); Application Interface”, ETSI GS QKD 004, V2.1.1, 2020.
- [174] ETSI, “Quantum Key Distribution (QKD); Control Interface for Software Defined Networks”, ETSI GS QKD 004, V2.1.1, 2022.
- [175] NSA, “Quantum Key Distribution (QKD) and Quantum Cryptography (QC)”, *Nsa.gov*, 2020. [En línea]. Disponible en: <https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC>. [Consultado: 19-oct-2024].
- [176] BSI, “Quantum Positionspapier”, *Bsi.bund.de*, 26-ene-2024. [En línea]. Disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html. [Consultado: 19-Oct-2024].
- [177] NCSC, “Quantum security technologies”, *Ncsc.gov.uk*, 2020. [En línea]. Disponible en: <https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies>. [Consultado: 19-Oct-2024].
- [178] ANSSI, “Should Quantum Key Distribution Be Used for Secure Communications?”, *Gouv.fr*, 2020. [En línea]. Disponible en: <https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be-used-secure-communications>. [Consultado: 19-oct-2024].
- [179] “PQCrypto Conferences”, *Pqcrypto.org*. [En línea]. Disponible en: <https://www.pqcrypto.org/conferences.html>. [Consultado: 15-nov-2024].
- [180] NIST, “Post-quantum cryptography FIPS approved”, NIST Computer Security Resource Center, 13-ago-2024. [En línea]. Disponible en: <https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved>. [Consultado: 15-nov-2024].
- [181] B. Schneier, “Threefish”, *Schneier on Security*, 10-dic-2015. [En línea]. Disponible en: <https://www.schneier.com/academic/skein/threefish>. [Consultado: 15-nov-2024].
- [182] P. Gaži y S. Tessaro, “Efficient and optimally secure key-length extension for block ciphers via randomized cascading”, en *Advances in Cryptology - EUROCRYPT 2012*, Springer Berlin Heidelberg, pp. 63–80, 2012.
- [183] R. Cramer y V. Shoup, “Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack”, *SIAM J. Comput.*, vol. 33, núm. 1, pp. 167–226, 2003.

- [184] T. Riastradh, “Public-key encryption (PKE)”, [Imagen]. Licencia Creative Commons: CC BY-SA 4.0. Disponible en: <https://en.wikipedia.org/wiki/File:PKE.svg>. [Accedido: 16-nov-2024].
- [185] T. Riastradh, “Key Encapsulation Mechanism”, [Imagen]. Licencia Creative Commons: CC BY-SA 4.0. Disponible en: <https://en.wikipedia.org/wiki/File:KEM.svg>. [Accedido: 16-nov-2024].
- [186] NIST, “Post-quantum cryptography - FAQs”, NIST Computer Security Resource Center. [En línea]. Disponible en: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs>. [Consultado: 16-nov-2024].
- [187] E. Fujisaki y T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes”, en *Advances in Cryptology - CRYPTO’ 99*, Springer Berlin Heidelberg, pp. 537–554, 1999.
- [188] D. T. Dam, T. H. Tran, V. P. Hoang, C. K. Pham, y T. T. Hoang, “A survey of post-quantum cryptography: Start of a new race”, *Cryptography*, vol. 7, núm. 3, p. 40, 2023.
- [189] NIST, “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”, NIST Computer Security Resource Center. [En línea]. Disponible en: <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf>. [Consultado: 17-nov-2024].
- [190] NIST, “Post-Quantum Cryptography – News and updates”, NIST Computer Security Resource Center, 03-ene-2017. [En línea]. Disponible en: <https://csrc.nist.gov/Projects/post-quantum-cryptography/news>. [Consultado: 16-nov-2024].
- [191] NIST, “Module-Lattice-Based Key-Encapsulation Mechanism Standard”, FIPS 203, 2024.
- [192] NIST, “Module-Lattice-Based Digital Signature Standard”, FIPS 204, 2024.
- [193] NIST, “Stateless Hash-Based Digital Signature Standard”, FIPS 205, 2024.
- [194] R. Bavdekar et al., “Post quantum cryptography: Techniques, challenges, standardization, and directions for future research”, arXiv:2202.02826 [cs.CR], 2022.
- [195] O. Goldreich, S. Goldwasser y S. Halevi, “Public-key cryptosystems from lattice reduction problems”, en *Advances in Cryptology - CRYPTO’ 97*, Springer Berlin Heidelberg, pp. 112–131, 1997.
- [196] J. Hoffstein, J. Pipher y J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem”, en *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, pp. 267–288, 1998.
- [197] C. Peikert, “A decade of lattice cryptography”, *Found. Trends Theor. Comput. Sci.*, vol. 10, núm. 4, pp. 283–424, 2016.
- [198] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography”, en *Proceedings of the 37th annual ACM symposium on Theory of computing*, pp. 84–93, 2005.
- [199] V. Lyubashevsky, C. Peikert, y O. Regev, “On ideal lattices and learning with errors over rings”, en *Advances in Cryptology – EUROCRYPT 2010*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 1–23.
- [200] Z. Brakerski, C. Gentry y V. Vaikuntanathan, “(Leveled) fully homomorphic encryption without bootstrapping”, *ACM Transactions of Computational Theory*, vol. 6, núm. 3, pp. 1–36, 2014.
- [201] A. Langlois y D. Stehlé, “Worst-case to average-case reductions for module lattices”, *Design, Codes and Cryptography*, vol. 75, núm. 3, pp. 565–599, 2015.
- [202] “Kyber”, Pq-crystals.org. [En línea]. Disponible en: <https://pq-crystals.org/kyber/index.shtml>. [Consultado: 30-nov-2024].
- [203] “SABER: LWR-based KEM”, Kuleuven.be. [En línea]. Disponible en: <https://www.esat.kuleuven.be/cosic/pqcrypto/saber/resources.html>. [Consultado: 30-nov-2024].
- [204] “FrodoKEM”, Frodokem.org. [En línea]. Disponible en: <https://frodokem.org>. [Consultado: 30-nov-2024].
- [205] “NTRU Prime: NISTPQC”, Cr.yo.to. [En línea]. Disponible en: <https://ntruprime.cr.yo.to/nist.html>. [Consultado: 30-nov-2024].

- [206] P. Schwabe, “Dilithium”, Pq-crystals.org. [En línea]. Disponible en: <https://pq-crystals.org/dilithium/index.shtml>. [Consultado: 30-nov-2024].
- [207] “Falcon”, Falcon-sign.info. [En línea]. Disponible en: <https://falcon-sign.info>. [Consultado: 30-nov-2024].
- [208] BSI, “Quantum-safe cryptography - fundamentals, current developments and recommendations”, Bsi.bund.de, 18-may-2022. [En línea]. Disponible en: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html>. [Consultado: 30-nov-2024].
- [209] R.J. McEliece, “A Public-Key Cryptosystem Based On Algebraic Coding Theory”, The Deep Space Network Progress Report, DSN PR 42-44, pp. 114-116, 1978.
- [210] H. Niederreiter, “Knapsack-type cryptosystems and algebraic coding theory”, Problems of Control and Information Theory, vol. 15, pp. 159–166, 1986.
- [211] “Classic McEliece: Intro”, Mceliece.org. [En línea]. Disponible en: <https://classic.mceliece.org/index.html>. [Consultado: 28-nov-2024].
- [212] “BIKE - bit flipping key encapsulation”, Bikesuite.org. [En línea]. Disponible en: <https://bikesuite.org>. [Consultado: 28-nov-2024].
- [213] “HQC”, Pqc-hqc.org. [En línea]. Disponible en: <https://pqc-hqc.org>. [Consultado: 28-nov-2024].
- [214] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc y J.-P. Tillich, “Structural cryptanalysis of McEliece schemes with compact keys”, Des. Codes Cryptogr., vol. 79, núm. 1, pp. 87–112, 2016.
- [215] M. Koochak Shooshtari et al., “Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes”, IET Information Security, vol. 10, núm. 4, pp. 194–202, 2016.
- [216] R. C. Merkle, “Secure communications over insecure channels”, Commun. ACM, vol. 21, núm. 4, pp. 294–299, 1978.
- [217] “PQCRainbow”, Pqcrainbow.org. [En línea]. Disponible en: <https://www.pqcrainbow.org>. [Consultado: 17-nov-2024].
- [218] “GeMSS”, Lip6.fr. [En línea]. Disponible en: <https://www.polsys.lip6.fr/Links/NIST/GeMSS.html>. [Consultado: 17-nov-2024].
- [219] C. Tao, A. Petzoldt y J. Ding, “Efficient key recovery for all HFE signature variants”, en Lecture Notes in Computer Science, Springer International Publishing, pp. 70–93, 2021.
- [220] W. Beullens, “Improved cryptanalysis of UOV and rainbow”, en Lecture Notes in Computer Science, Springer International Publishing, pp. 348–373, 2021.
- [221] W. Beullens, “Breaking Rainbow takes a weekend on a laptop”, en Advances in Cryptology – CRYPTO 2022, Springer Nature Switzerland, pp. 464–479, 2022.
- [222] J. Baena et al., “Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow”, en Advances in Cryptology – CRYPTO 2022. Lecture Notes in Computer Science, vol. 13.509, pp. 376–405, 2022.
- [223] “SIKE – supersingular isogeny key encapsulation”, SIKE – Supersingular Isogeny Key Encapsulation. [En línea]. Disponible en: <https://sike.org>. [Consultado: 17-nov-2024].
- [224] W. Castryck y T. Decru, “An Efficient Key Recovery Attack on SIDH”, en Advances in Cryptology – EUROCRYPT 2023, Lecture Notes in Computer Science, vol. 14.008, pp. 423–447, 2023.
- [225] NIST, “Chapter 0. Foreword and postscript”, NIST Computer Security Resource Center. [En línea]. Disponible en: <https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf>. [Consultado: 17-nov-2024].
- [226] G. Zaverucha et al., “Picnic Signature Scheme”. Github.io [En línea]. Disponible en: <https://microsoft.github.io/Picnic>. [Consultado: 17-nov-2024].

- [227] S. Banik, A. Caforio y S. Vaudenay, “New attacks on LowMC using partial sets in the single-data setting”, IACR Communications in Cryptology, vol. 1, 2024.
- [228] M. Ajtai, “Generating hard instances of lattice problems (extended abstract)”, en Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96, 1996.
- [229] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, y D. Stehlé, “Classical hardness of learning with errors”, en Proceedings of the forty-fifth annual ACM symposium on Theory of Computing, 2013.
- [230] A. Shaller, L. Zamir y M. Nojoumian, “Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures”, Inf. Comput., vol. 295, núm. 105112, p. 105112, 2023.
- [231] T. Kamucheka, M. Fahr, T. Teague, A. Nelson, D. Andrews y M. Huang, “Power-based side channel attack analysis on PQC algorithms”, IACR Cryptol eprint archive, vol. 2021, p. 1021, 2021.
- [232] C. Mújdei, L. Wouters, A. Karmakar, A. Beckers, J. M. B. Mera y I. Verbauwhede, “Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication”, ACM Trans. Embed. Comput. Syst., 2022.
- [233] Y. Tanaka, R. Ueno, K. Xagawa, A. Ito, J. Takahashi y N. Homma, “Multiple-valued plaintext-checking side-channel attacks on post-quantum KEMs”, IACR Cryptol eprint Arch, vol. 2022, p. 940, 2023.
- [234] B. Seck et al., “A side-channel attack against classic McEliece when loading the goppa polynomial”, en Lecture Notes in Computer Science, Springer Nature Switzerland, pp. 105–125, 2023.
- [235] G. Goy, A. Loiseau, y P. Gaborit, “A new key recovery side-channel attack on HQC with chosen ciphertext”, en Post-Quantum Cryptography, Springer International Publishing, pp. 353–371, 2022.
- [236] Y. Chen, “Quantum algorithms for lattice problems”, IACR Cryptol eprint Arch, vol. 2024, p. 555, 2024.
- [237] B. Schneier, “Lattice-based cryptosystems and quantum cryptanalysis”, Communications ACM, 2024.
- [238] D. Bernstein, “cr.y.p.to: 2024.01.02: Double encryption”, Cr.y.p.to, 2-ene-2024. [En línea]. Disponible en: <https://blog.cr.y.p.to/20240102-hybrid.html>. [Consultado: 23-nov-2024].
- [239] S. Schmieg, S. Kölbl y G. Endignoux, “Blog: Google’s Threat model for Post-Quantum Cryptography”, Google.com, 11-mar-2024. [En línea]. Disponible en: <https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography>. [Consultado: 23-nov-2024].
- [240] S. Kölbl, S. Schmieg y G. Endignoux, “Blog: Why hybrid deployments are key to secure PQC migration”, Google.com, 21-mar-2024. [En línea]. Disponible en: <https://bughunters.google.com/blog/5266882047639552/why-hybrid-deployments-are-key-to-secure-pqc-migration>. [Consultado: 23-nov-2024].
- [241] K. Kwiatkowski, “The TLS post-quantum experiment”, The Cloudflare Blog, 30-oct-2019. [En línea]. Disponible en: <https://blog.cloudflare.com/the-tls-post-quantum-experiment>. [Consultado: 02-dic-2024].
- [242] Defense.gov. “The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ”, National Security Agency Cybersecurity Information Sheet, abr-2024. [En línea]. Disponible en: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF. [Consultado: 23-nov-2024].
- [243] NIST, “Recommendation for Key Management: Part 1. General”, NIST SP 800-57 Part 1 Rev. 5, 2020.
- [244] F. Opiłka, M. Niemiec, M. Gagliardi, y M. A. Kourtis, “Performance analysis of post-quantum cryptography algorithms for digital signature”, Appl. Sci. (Basel), vol. 14, núm. 12, p. 4994, 2024.
- [245] “Liboqs”, Open Quantum Safe. [En línea]. Disponible en: <https://openquantumsafe.org/liboqs>. [Consultado: 23-nov-2024].

- [246] M. Ounsworth, J. Gray, M. Pala, J. Klaußner y S. Fluhrer, “Composite ML-DSA for use in X.509 public key infrastructure and CMS”, IETF Datatracker. [En línea]. Disponible en: <https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs>. [Consultado: 23-nov-2024].
- [247] P. Hoffman y J. Schaad, “New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)”, RFC 5912, jun-2010. [En línea]. Disponible en: <https://datatracker.ietf.org/doc/rfc5912>. [Consultado: 23-nov-2024].
- [248] R. Housley, “Cryptographic Message Syntax (CMS)”, RFC 5652, sep-2009. [En línea]. Disponible en: <https://www.rfc-editor.org/info/rfc5652>. [Consultado: 23-nov-2024].
- [249] N. Bindel y B. Hale, “A Note on Hybrid Signature Schemes”, Iacr.org. [En línea]. Disponible en: <https://eprint.iacr.org/2023/423.pdf>. [Consultado: 02-dic-2024].
- [250] H.-Y. Kwon, I. Bajuna y M.-K. Lee, “Compact hybrid signature for secure transition to post-quantum era”, IEEE Access, vol. 12, pp. 39.417-39.429, 2024.
- [251] M. Friedl, J. Mojzis, y S. Josefsson, “Secure Shell (SSH) key exchange method using hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: Sntrup761x25519-sha512”, IETF Datatracker. [En línea]. Disponible en: <https://datatracker.ietf.org/doc/draft-ietf-sshm-ntruprime-ssh>. [Consultado: 01-dic-2024].
- [252] “KEM performance”, Openquantumsafe.org. [En línea]. Disponible en: https://openquantumsafe.org/benchmarking/visualization/speed_kem.html. [Consultado: 01-dic-2024].
- [253] B. Westerbaan, “NIST’s pleasant post-quantum surprise”, The Cloudflare Blog, 08-jul-2022. [En línea]. Disponible en: <https://blog.cloudflare.com/nist-post-quantum-surprise>. [Consultado: 01-dic-2024].
- [254] “REPORT ON POST-QUANTUM CRYPTOGRAPHY. As required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No: 117-260”, Whitehouse.gov, july-2024. [En línea]. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf. [Consultado: 09-dic-2024].
- [255] S. Fluhrer, P. Kampanakis, D. McGrew y V. Smyslov, “Mixing preshared keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for post-quantum security”, RFC 8784, ene-2020. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc8784>. [Consultado: 05-ene-2025].
- [256] R. Singh, C. Hill, S. Kawaguchi y J. Lupo, “Secure Key Integration Protocol (SKIP)”, Ietf.org, ago-2024. [En línea]. Disponible en: <https://www.ietf.org/archive/id/draft-cisco-skip-00.html>. [Consultado: 05-ene-2025].
- [257] “Telefonica, Fortinet and ID Quantique (IDQ) have jointly demonstrated the first Quantum-Safe IPVPN connection suitable for offering a fully managed datacenter interconnection service”, Telefónica, oct-2021. [En línea]. Disponible en: <https://www.telefonica.com/en/communication-room/blog/telefonica-fortinet-and-id-quantique-idq-have-jointly-demonstrated-the-first-quantum-safe-ipvpn-connection-suitable-for-offering-a-fully-managed-datacenter-interconnection-service>. [Consultado: 05-ene-2025].
- [258] T. Reddy, V. Smyslov y S. Fluhrer, “Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC”, Ietf.org, nov-2024. [En línea]. Disponible en: <https://www.ietf.org/archive/id/draft-reddy-ipsecme-ikev2-pqc-auth-03.txt>. [Consultado: 10-ene-2025].
- [259] T. Reddy, T. Hollebeek, J. Gray, y S. Fluhrer, “Use of composite ML-DSA in TLS 1.3”, IETF Datatracker, nov-2024. [En línea]. Disponible en: <https://datatracker.ietf.org/doc/html/draft-tls-reddy-composite-mldsa>. [Consultado: 10-ene-2025].
- [260] “SSH”, Open Quantum Safe. [En línea]. Disponible en: <https://openquantumsafe.org/applications/ssh.html>. [Consultado: 10-ene-2025].
- [261] P. Kampanakis, D. Stebila, y T. Hansen, “Post-quantum hybrid key exchange in SSH”, Ietf.org, nov-2022. [En línea]. Disponible en: <https://www.ietf.org/archive/id/draft-kampanakis-curdle-ssh-pq-ke-00.html>. [Consultado: 10-ene-2025].
- [262] “Quantum resistance and the Signal Protocol”, Signal Messenger, 19-sep-2023. [En línea]. Disponible en: <https://signal.org/blog/pqxdh>. [Consultado: 10-ene-2025].

- [263] “The X3DH key agreement protocol”, Signal Messenger, 4-nov-2016. [En línea]. Disponible en: <https://signal.org/docs/specifications/x3dh>. [Consultado: 10-ene-2025].
- [264] “iMessage with PQ3: The new state of the art in quantum-secure messaging at scale”, Apple Security Research, 21-feb-2024. [En línea]. Disponible en: <https://security.apple.com/blog/imessage-pq3>. [Consultado: 10-ene-2025].
- [265] A. Hülsing, K.-C. Ning, P. Schwabe, F. J. Weber y P. R. Zimmermann, “Post-quantum WireGuard”, en IEEE Symposium on Security and Privacy (SP), 2021.
- [266] Y. Angel, B. Dowling, A. Hülsing, P. Schwabe y F. Weber, “Post Quantum Noise”, en Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 2022.
- [267] C. J. Tjhai et al., “Multiple key exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)”, RFC 9370, may-2023. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc9370>. [Consultado: 09-ene-2025].
- [268] “Palo Alto networks extends support for quantum safe VPN with RFC 9242, RFC 9370 standards, and hybrid KEYS”, Paloaltonetworks.com, 02-may-2024. [En línea]. Disponible en: <https://live.paloaltonetworks.com/t5/community-blogs/palo-alto-networks-extends-support-for-quantum-safe-vpn-with-rfc/ba-p/585492>. [Consultado: 10-ene-2025].
- [269] “Configure a Site-to-Site IKEv2 tunnel between two ASAs using IKEv2 Multiple Key Exchanges”, Cisco, 16-ene-2024. [En línea]. Disponible en: <https://www.cisco.com/c/en/us/support/docs/security-vpn/internet-security-association-key-management-protocol-isakmp/221560-configure-a-site-to-site-ikev2-tunnel-be.html>. [Consultado: 10-ene-2025].
- [270] “Enhancing security with Post-Quantum Cryptography for IPsec key exchange 7.6.1”, Fortinet.com. [En línea]. Disponible en: <https://docs.fortinet.com/document/fortigate/7.6.0/new-features/229631/enhancing-security-with-post-quantum-cryptography-for-ipsec-key-exchange-7-6-1>. [Consultado: 10-ene-2025].
- [271] P. Kampanakis y G. Ravago, “Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)”, Ietf.org, nov-2024. [En línea]. Disponible en: <https://www.ietf.org/archive/id/draft-kampanakis-ml-kem-ikev2-09.txt>. [Consultado: 09-ene-2025].
- [272] G. Wang, “Post-quantum hybrid key exchange in the IKEv2 with FrodoKEM”, IETF Datatracker, oct-2024. [En línea]. Disponible en: <https://datatracker.ietf.org/doc/html/draft-wang-hybrid-kem-ikev2-frodo-02>. [Consultado: 09-ene-2025].
- [273] Cloudflare.com. [En línea]. Disponible en: <https://blog.cloudflare.com/content/images/2022/10/image3.png>. [Consultado: 09-ene-2025].
- [274] D. Stebila, S. Fluhrer y S. Gueron, “Hybrid key exchange in TLS 1.3”, Ietf.org, oct-2024. [En línea]. Disponible en: <https://www.ietf.org/archive/id/draft-ietf-tls-hybrid-design-11>. [Consultado: 11-ene-2025].
- [275] B. E. Westerbaan y D. Stebila, “X25519Kyber768Draft00 hybrid post-quantum key agreement”, Ietf.org, sept-2023. [En línea]. Disponible en: <https://www.ietf.org/archive/id/draft-tls-westerbaan-xyber768d00-03>. [Consultado: 11-ene-2025].
- [276] “Protecting chrome traffic with hybrid kyber KEM”, Chromium Blog, ago-2023. [En línea]. Disponible en: <https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html>. [Consultado: 11-ene-2025].
- [277] B. Westerbaan, “Defending against future threats: Cloudflare goes post-quantum”, The Cloudflare Blog, 03-oct-2022. [En línea]. Disponible en: <https://blog.cloudflare.com/post-quantum-for-all>. [Consultado: 11-ene-2025].
- [278] H. Krawczyk y P. Eronen, “HMAC-based Extract-and-Expand Key Derivation Function (HKDF)”, RFC 5869, may-2010. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc5869>. [Consultado: 11-ene-2025].
- [279] “TLS 1.3 Hybrid Key Exchange using X25519Kyber768 / ML-KEM”, Netmeister.org, oct-2024. [En línea]. Disponible en: <https://www.netmeister.org/blog/tls-hybrid-kex.html>. [Consultado: 11-ene-2025].

- [280] J. Henrich, A. Heinemann, A. Wiesmaier y N. Schmitt, “Performance impact of PQC KEMs on TLS 1.3 under varying network characteristics”, en *Lecture Notes in Computer Science*, Springer Nature Switzerland, pp. 267–287, 2023.
- [281] “TLS”, Open Quantum Safe. [En línea]. Disponible en: <https://openquantumsafe.org/applications/tls.html>. [Consultado: 11-ene-2025].

9 ACRÓNIMOS

AE	Authenticated Encryption
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AKE	Authentication and Key Establishment
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (Francia)
API	Application Programming Interface
BIKE	Bit Flipping Key Encapsulation
BSI	Bundesamt für Sicherheit in der Informationstechnik (Alemania)
CA	Certificate Authority
CBC	Cipher Block Chaining
CCA	Chosen Ciphertext Attack
CCA2	Chosen Ciphertext Attack Adaptative
CCM	Counter with Cipher Block Chaining
CMAC	Cipher-based Message Authentication Code
COA	Ciphertext Only Attack
COW	Coherent One Way
CPA	Chosen Plaintext Attack
CPA2	Chosen Plaintext Attack Adaptative
CRL	Certificate Revocation List
CRQC	Cryptographically Relevant Quantum Computer
CTR	Counter mode
CVP	Closest Vector Problem
CV-QKD	Continuous Variable Quantum Key Distribution
DES	Data Encryption Standard
DH	Diffie Hellman
DoS	Denial of Service
DPS	Differential Phase Shift
DS	Digital Signature
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
DV-QKD	Discrete Variable Quantum Key Distribution
ECC	Elliptic Curve Cryptography

ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards curve Digital Signature Algorithm
EEUU	Estados Unidos de América
EK	Ephemeral Key
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
EUUF-CMA	Existential Unforgeability under Chosen Message Attack
FALCON	Fast Fourier Lattice-based Compact Signatures
FIPS	Federal Information Processing Standards
GapSVP	Gap Shortest Vector Problem
GCM	Galois Counter Mode
GeMSS	Geometrically Multivariate Signature Scheme
GEO	Geostationary Earth Orbit
GNFS	General Number Field Sieve
HDQKD	High-dimensional quantum key distribution
HKDF	HMAC-based Key Derivation Function
HMAC	Hash-based Message Authentication Code
HQC	Hamming Quasi-Cyclic
IBM	International Business Machines Corporation
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IND-CCA2	Indistinguishability under Chosen Ciphertext Attack, level 2
IND-CPA	Indistinguishability under Chosen Plaintext Attack
IoT	Internet of Things
IP	Internet Protocol
IPSEC	Internet Protocol SECurity
KEM	Key Encapsulation Mechanism
KM	Key Manager
KMS	Key Management System
KPA	Known Plaintext Attack
LEO	Low Earth Orbit
LWE	Learning With Errors
LTK	Long Term Key

MAC	Message Authentication Code
MIT	Massachusetts Institute of Technology
MITM	Man In The Middle
med	Máximo común divisor
ML-DSA	Modular Lattice-based Digital Signature Algorithm
ML-KEM	Modular Lattice-based Key Encapsulation Mechanism
M-LWE	Modular Learning With Errors
MTU	Maximum Transmission Unit
NCSC	National Cyber Security Centre (Reino Unido)
NIST	National Institute of Standards and Technology (EEUU)
NSA	National Security Agency (EEUU)
OTP	One Time Pad
PFS	Perfect Forward Secrecy
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PRF	Pseudo-Random Function
PSK	Pre-Shared Key
QC	Quantum Computing
QCI	Quantum Communications Infrastructure
QKD	Quantum Key Distribution
QoS	Quality of Service
QRNG	Quantum Random Number Generation
QUIC	Quick UDP Internet Connections
REST	REpresentational State Transfer
RFC	Request For Comments
R-LWE	Ring Learning With Error
RSA	Rivest, Shamir & Adleman
SA	Security Association
SDN	Software Defined Network
SIKE	Supersingular Isogeny Key Encapsulation
SIM	Subscriber Identify Module
SIVP	Shortest Integer Vector Problem

SK	Session Key
SKIP	Secure Key Integration Protocol
SLH-DSA	StateLess Hash-based Digital Signature Algorithm
SPHINCS+	Stateless Practical Hash-Based Signature Scheme Plus
SSH	Secure Shell
SVP	Short Vector Problem
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTP	Trusted Third Party
USIM	Universal Subscriber Identify Module

