Criptografía bajo una Nueva Luz: De la Certidumbre Clásica a las Revoluciones Cuánticas

Sección I: Los Fundamentos de la Confianza en un Mundo Digital

1.1 Definiendo la Criptografía: La Ciencia de la Comunicación Segura

La criptografía es la disciplina que encarna los principios, medios y métodos para la transformación de datos con el fin de ocultar su contenido semántico, prevenir su uso no autorizado o evitar su modificación no detectada.[1] Históricamente, sus raíces se encuentran en la necesidad de enviar información sensible entre figuras militares y políticas, donde el objetivo principal era mantener el secreto de los mensajes.[2] Sin embargo, la criptografía moderna ha evolucionado desde este enfoque inicial en la "escritura secreta" para convertirse en una ciencia integral de la seguridad de la información, que abarca un espectro mucho más amplio de objetivos y aplicaciones.[3]
En el contexto contemporáneo, la criptografía protege la información en todos sus estados: en reposo (como un archivo en un disco duro), en tránsito (como las comunicaciones electrónicas intercambiadas entre dos o más partes) y en uso (mientras se realizan cálculos sobre los datos).[2] Su importancia es tal que se ha convertido en la tecnología fundamental que sustenta la sociedad digital moderna. Es la base de innumerables aplicaciones de Internet a través del Protocolo Seguro de Transferencia de Hipertexto (HTTPS), las comunicaciones seguras de texto y voz, el comercio electrónico, las tarjetas de pago basadas en chips e incluso las monedas digitales.[2]

1.2 Los Cuatro Pilares de la Seguridad de la Información

A medida que la seguridad ha avanzado, el campo de la criptografía se ha expandido para

incluir un conjunto más amplio de objetivos de seguridad. La evolución de los objetivos centrales de la criptografía, desde la simple confidencialidad a un conjunto integral de cuatro servicios de seguridad, no es una mera expansión académica, sino una consecuencia causal directa de la creciente complejidad y los requisitos de confianza de la sociedad digital moderna. La criptografía primitiva se centraba casi exclusivamente en la confidencialidad de los mensajes.[2] Con el advenimiento del comercio digital y las interacciones legales en línea, se hizo evidente que el secreto por sí solo era insuficiente. Era necesario garantizar que los detalles de una transacción no pudieran ser alterados (integridad), que las partes fueran quienes decían ser (autenticación) y que una transacción no pudiera ser negada posteriormente (no repudio). Cada nuevo pilar de la seguridad se desarrolló para replicar y hacer cumplir un componente de la confianza que se da por sentado en las interacciones cara a cara. Estos cuatro pilares son:

- **Confidencialidad:** Asegura que la información solo esté disponible para los usuarios autorizados. Este es el objetivo más comúnmente abordado y se logra principalmente a través del cifrado, el proceso de convertir un mensaje de texto plano en un texto cifrado ininteligible.[2]
- **Integridad:** Garantiza que la información no ha sido manipulada o alterada durante su almacenamiento o transmisión. Este objetivo se logra típicamente mediante el uso de funciones hash criptográficas, que crean una "huella digital" única para los datos.[2]
- **Autenticación:** Confirma la autenticidad de la información o la identidad de un usuario. Permite a un remitente y a un destinatario verificar la identidad del otro y el destino del mensaje, a menudo mediante el uso de certificados digitales y firmas digitales.[2]
- **No Repudio:** Impide que un usuario niegue compromisos o acciones previas. Proporciona una prueba irrefutable de que un usuario específico envió un mensaje o realizó una transacción, una función clave de las firmas digitales.[2]

1.3 La Dicotomía Clásico-Cuántica: Una Visión General del Cambio de Paradigma

El edificio de la criptografía se asienta sobre dos cimientos fundamentalmente distintos, que definen la era actual y la futura de la seguridad de la información.

- **Fundamento de la Criptografía Clásica:** La seguridad de los sistemas criptográficos actuales, como RSA y la criptografía de curva elíptica (ECC), se basa en la dificultad computacional de ciertos problemas matemáticos. Estos problemas, como la factorización de números enteros grandes o el cálculo de logaritmos discretos, se consideran intratables para las computadoras clásicas, requiriendo escalas de tiempo que superan la edad del universo para su resolución.[7] La confianza en estos sistemas es, por tanto, una confianza en la limitación del poder computacional.
- **Fundamento de la Criptografía Cuántica:** En contraste, un nuevo paradigma de

seguridad emerge de las leyes fundamentales e inmutables de la física cuántica. La criptografía cuántica no depende de la dificultad matemática, sino de principios como el efecto observador (Principio de Incertidumbre de Heisenberg), que dicta que el acto de medir un sistema cuántico lo perturba de forma detectable, y el teorema de no clonación, que prohíbe la creación de una copia idéntica de un estado cuántico desconocido.[7] La seguridad, en este caso, está garantizada por la propia naturaleza.

Este informe explorará la profunda tensión y la fascinante sinergia entre estos dos mundos. Se detallará cómo los principios de la mecánica cuántica, cuando se aprovechan en una computadora cuántica, amenazan con demoler los cimientos matemáticos de la criptografía clásica. Simultáneamente, se examinará cómo esos mismos principios ofrecen una base completamente nueva y físicamente robusta para la seguridad, marcando el comienzo de una revolución criptográfica.

Sección II: La Mecánica de la Criptografía Clásica

Los métodos criptográficos se pueden clasificar en tres tipos principales: criptografía de clave simétrica, criptografía de clave asimétrica y funciones hash.[3] Cada uno de estos opera bajo principios distintos y sirve para propósitos complementarios dentro de un ecosistema de seguridad robusto. La evolución de estos métodos no ha sido un proceso de simple reemplazo, sino de síntesis. Las limitaciones inherentes de un paradigma criptográfico han catalizado directamente la invención del siguiente, culminando en la arquitectura híbrida que domina los sistemas seguros modernos como TLS/SSL. Este desarrollo revela una clara trayectoria evolutiva de causa y efecto en el diseño criptográfico, donde la combinación de diferentes enfoques no es simplemente una opción, sino una necesidad arquitectónica.

2.1 Criptografía de Clave Simétrica: El Secreto Compartido

- **Principio de Operación:** La criptografía de clave simétrica, también conocida como criptografía de clave secreta, utiliza una única clave compartida tanto para el cifrado como para el descifrado de datos.[3] Ambas partes de la comunicación deben poseer la misma clave secreta.
- **Fortalezas y Debilidades:** La principal ventaja de la criptografía simétrica es su velocidad y eficiencia computacional. Requiere menos recursos y es significativamente más rápida que la criptografía asimétrica, lo que la hace ideal para cifrar grandes volúmenes de datos, como archivos o flujos de comunicación continuos.[12] Su debilidad fundamental reside en el problema de la distribución de claves: la clave secreta debe ser compartida de forma segura entre las partes antes de que pueda comenzar la comunicación segura. Si un adversario intercepta la clave durante este intercambio,

toda la seguridad del sistema se ve comprometida.[3]

- Análisis en Profundidad: El Estándar de Cifrado Avanzado (AES)
  El AES es el estándar de cifrado simétrico más utilizado en el mundo, adoptado por el gobierno de los EE. UU. y utilizado globalmente para proteger datos sensibles.16
    - **Estructura del Algoritmo:** AES es un cifrado por bloques que opera sobre bloques de datos de tamaño fijo de 128 bits. Su diseño se basa en una red de sustitución-permutación (SPN), que es más eficiente en hardware y software que la red de Feistel utilizada por su predecesor, DES.[16]
    - **Tamaños de Clave:** El estándar soporta tres tamaños de clave: 128, 192 y 256 bits. El número de rondas de cifrado depende del tamaño de la clave: 10 rondas para claves de 128 bits, 12 para 192 bits y 14 para 256 bits.[16]
    - **Operaciones de Ronda:** Cada ronda de cifrado (excepto la última) consiste en cuatro transformaciones distintas que se aplican al bloque de datos, conocido como el "estado":
        1. SubBytes: Es un paso de sustitución no lineal donde cada byte del estado se reemplaza por otro según una tabla de consulta predeterminada llamada S-box. Esta operación introduce confusión en el cifrado, oscureciendo la relación entre la clave y el texto cifrado.[16]
        2. ShiftRows: Un paso de transposición en el que las filas del estado se desplazan cíclicamente un cierto número de pasos. Esto proporciona difusión, asegurando que las redundancias en el texto plano se distribuyan por todo el texto cifrado.[16]
        3. MixColumns: Una operación de mezcla lineal que opera en las columnas del estado, combinando los cuatro bytes de cada columna. Este paso aumenta aún más la difusión.[16] Esta operación se omite en la ronda final.
        4. AddRoundKey: Cada byte del estado se combina con una "clave de ronda" mediante una operación XOR bit a bit. Las claves de ronda se derivan de la clave de cifrado principal a través de un proceso de expansión de clave (KeyExpansion).[16]

2.2 Criptografía de Clave Asimétrica: El Par de Claves Pública-Privada

- **Principio de Operación:** La criptografía de clave asimétrica, o criptografía de clave pública, utiliza un par de claves matemáticamente relacionadas: una clave pública y una clave privada.[3] La clave pública se puede distribuir libremente y se utiliza para cifrar datos. La clave privada, que se mantiene en secreto por su propietario, es la única que puede descifrar los datos cifrados con la clave pública correspondiente.
- **Fortalezas y Debilidades:** La principal fortaleza de este método es que resuelve elegantemente el problema de la distribución de claves de la criptografía simétrica.[14]

Además, permite la creación de firmas digitales, que son cruciales para la autenticación y el no repudio.[2] Su principal debilidad es su lentitud y alta carga computacional en comparación con los métodos simétricos, lo que la hace inadecuada para cifrar grandes cantidades de datos.[12]

- Análisis en Profundidad: El Algoritmo RSA
  Nombrado por sus inventores Rivest, Shamir y Adleman, el RSA es el algoritmo de clave asimétrica más conocido y utilizado.8
  - **Fundamento Matemático:** Su seguridad se basa en la dificultad computacional de factorizar el producto de dos números primos grandes. Es fácil multiplicar dos primos, pero extremadamente difícil determinar los factores primos originales a partir de su producto.[8]
  - **Generación de Claves:** El proceso implica los siguientes pasos:
    1. Seleccionar dos números primos grandes y aleatorios, p y q.
    2. Calcular su producto, el módulo $n=pq$.
    3. Calcular la función totiente de Euler: $\varphi(n)=(p-1)(q-1)$.
    4. Elegir un entero e (el exponente público) tal que $1<e<\varphi(n)$ y e sea coprimo con $\varphi(n)$.
    5. Calcular d (el exponente privado) como el inverso multiplicativo de e módulo $\varphi(n)$, de modo que $d \cdot e \equiv 1 \pmod{\varphi(n)}$.
    6. La clave pública es el par (n,e) y la clave privada es el par (n,d).[20]
  - **Proceso de Cifrado y Descifrado:**
    - **Cifrado:** Para cifrar un mensaje m, se calcula el texto cifrado c como: $c=m^e \pmod n$.
    - **Descifrado:** Para descifrar c, se calcula el mensaje original m como: $m=c^d \pmod n$.[20]
  - **Cifrado Híbrido en la Práctica:** La lentitud de RSA lo hace impráctico para cifrar directamente grandes volúmenes de datos. En aplicaciones del mundo real como los protocolos TLS/SSL que aseguran la web, se utiliza un enfoque híbrido. La criptografía asimétrica (RSA) se usa para un propósito muy específico: cifrar y intercambiar de forma segura una clave simétrica (como una clave AES) generada para una sesión de comunicación única. Una vez que ambas partes comparten de forma segura esta "clave de sesión", utilizan la criptografía simétrica (AES), mucho más rápida, para cifrar el resto de la comunicación.[12]

2.3 Funciones Hash Criptográficas: La Huella Digital

- **Principio de Operación:** Una función hash criptográfica es un algoritmo que toma una entrada de tamaño arbitrario (un mensaje, un archivo, etc.) y produce una salida de tamaño fijo, conocida como hash o resumen (digest).[2]

- **Propiedades Fundamentales:** Para ser criptográficamente segura, una función hash debe poseer tres propiedades clave:
    1. **Resistencia a la preimagen (unidireccionalidad):** Dado un hash h, debe ser computacionalmente inviable encontrar una entrada m tal que hash(m)=h.[26]
    2. **Resistencia a la segunda preimagen:** Dada una entrada m1, debe ser computacionalmente inviable encontrar una entrada diferente m2 tal que hash(m1)=hash(m2).
    3. **Resistencia a colisiones:** Debe ser computacionalmente inviable encontrar dos entradas distintas cualesquiera, m1 y m2, tales que hash(m1)=hash(m2).[26]
- **Aplicaciones:** Las funciones hash son fundamentales para verificar la integridad de los datos, almacenar contraseñas de forma segura (almacenando el hash de la contraseña en lugar de la contraseña misma) y son un componente esencial de los algoritmos de firma digital.[2]
- Análisis en Profundidad: El Algoritmo de Hash Seguro (SHA-256)
  SHA-256 es un miembro de la familia de algoritmos SHA-2 y es ampliamente utilizado en protocolos de seguridad y criptomonedas como Bitcoin.26
    - **Salida:** Genera un valor hash de 256 bits (32 bytes).[24]
    - **Preprocesamiento:** El mensaje de entrada se procesa para asegurar que su longitud sea un múltiplo de 512 bits. Esto implica: 1) añadir un bit '1' al final del mensaje; 2) añadir bits '0' (padding) hasta que la longitud del mensaje sea 64 bits menor que un múltiplo de 512; 3) añadir los 64 bits restantes para representar la longitud del mensaje original en bits.[25]
    - **Inicialización:** El algoritmo opera con un estado interno de 256 bits, representado por ocho variables de 32 bits (h0 a h7). Estas se inicializan con valores constantes predefinidos, que son las primeras 32 bits de las partes fraccionarias de las raíces cuadradas de los primeros ocho números primos.[26]
    - **Bucle de Compresión:** El mensaje preprocesado se divide en bloques de 512 bits. El algoritmo procesa cada bloque secuencialmente, utilizando cada uno para actualizar el estado interno. Este proceso se realiza en 64 rondas de operaciones complejas que incluyen funciones lógicas bit a bit, adiciones modulares y rotaciones. El resultado de procesar un bloque se convierte en el estado inicial para el siguiente. El valor hash final es la concatenación de los valores de las ocho variables de estado después de procesar el último bloque.

Sección III: La Revolución Cuántica y sus Consecuencias Criptográficas

A principios del siglo XX, la física clásica, que había descrito con éxito el mundo

macroscópico durante siglos, se encontró con una serie de fenómenos a escala atómica que no podía explicar. Estas anomalías no eran simples detalles, sino profundas contradicciones que exigían un cambio de paradigma radical, dando lugar al nacimiento de la mecánica cuántica. Este nuevo marco no solo redefinió nuestra comprensión de la realidad, sino que también sentó las bases para una nueva forma de computación con el poder de deshacer las garantías de seguridad de la criptografía clásica.

3.1 Los Límites de la Física Clásica: Una Partida Necesaria

Dos fenómenos clave marcaron el colapso de la física clásica y el amanecer de la era cuántica:

- **Radiación de Cuerpo Negro y la Catástrofe Ultravioleta:** La física clásica, a través de la ley de Rayleigh-Jeans, predecía que un objeto ideal que absorbe toda la radiación incidente (un "cuerpo negro") debería emitir una cantidad infinita de energía a altas frecuencias (en el rango ultravioleta). Esta predicción, conocida como la "catástrofe ultravioleta", estaba en flagrante contradicción con las observaciones experimentales, que mostraban que la energía emitida alcanzaba un pico y luego disminuía a cero en las altas frecuencias.[28] En 1900, Max Planck resolvió este enigma con una propuesta revolucionaria: la energía no se emite de forma continua, sino en paquetes discretos o "cuantos". Postuló que la energía de cada cuanto era directamente proporcional a su frecuencia, dada por la ecuación
  $E=hv$, donde h es una nueva constante fundamental, ahora conocida como la constante de Planck.[32] Esta idea de la cuantización de la energía fue el primer postulado de la teoría cuántica y ajustaba perfectamente los datos experimentales.
- **El Efecto Fotoeléctrico:** Otro misterio era el efecto fotoeléctrico, donde la luz que incide sobre una superficie metálica puede expulsar electrones. La teoría ondulatoria clásica de la luz predecía que la energía de los electrones expulsados debería depender de la intensidad (brillo) de la luz. Sin embargo, los experimentos mostraron que la energía de los electrones dependía únicamente de la frecuencia (color) de la luz, y que no se emitían electrones por debajo de una frecuencia umbral, sin importar cuán intensa fuera la luz.[31] En 1905, Albert Einstein, extendiendo la idea de Planck, propuso que la luz misma está compuesta de partículas discretas de energía, más tarde llamadas fotones, cada una con una energía
  $E=hv$. Esta visión corpuscular de la luz explicaba perfectamente el fenómeno: un fotón transfiere toda su energía a un solo electrón. Si la energía del fotón es suficiente para superar la "función de trabajo" del metal (la energía que liga al electrón), el electrón es expulsado. Cualquier energía sobrante se convierte en la energía cinética del electrón.[36]

3.2 Principios Fundamentales del Mundo Cuántico

La mecánica cuántica describe un mundo regido por reglas extrañas y antiintuitivas que no tienen análogo en nuestra experiencia macroscópica.

- **Dualidad Onda-Partícula:** En el corazón de la mecánica cuántica se encuentra la idea de que las entidades subatómicas, como los electrones y los fotones, no son ni ondas ni partículas en el sentido clásico. Exhiben comportamientos de ambos tipos dependiendo del experimento que se realice.[45] El famoso experimento de la doble rendija demuestra esto de manera concluyente: cuando se envían electrones uno por uno hacia una barrera con dos rendijas, cada electrón impacta en una pantalla detectora como una partícula localizada. Sin embargo, con el tiempo, el patrón de impactos acumulados revela un patrón de interferencia, una firma característica de las ondas que pasan por ambas rendijas simultáneamente e interfieren consigo mismas.[46] Louis de Broglie generalizó esta idea al postular que toda la materia tiene una longitud de onda asociada, dada por la relación
  $\lambda = h/p$, donde p es el momento de la partícula.[48]
- **Superposición:** Antes de una medición, un sistema cuántico puede existir en una combinación lineal de todos sus estados posibles simultáneamente. Este principio de superposición se representa matemáticamente describiendo el estado de un sistema, $|\psi\rangle$, como un vector en un espacio de Hilbert complejo. Si $|estado1\rangle$ y $|estado2\rangle$ son dos estados posibles, el sistema puede estar en el estado superpuesto $|\psi\rangle = c1|estado1\rangle + c2|estado2\rangle$.[51] Los coeficientes
  c1 y c2 son números complejos llamados amplitudes de probabilidad. El acto de medir el sistema lo obliga a "colapsar" en uno de los estados base, y la probabilidad de obtener, por ejemplo, estado1 está dada por el cuadrado del módulo de su amplitud, $P1 = |c1|2$.[33]
- **Entrelazamiento:** Quizás el fenómeno cuántico más desconcertante es el entrelazamiento, que Einstein describió como "acción fantasmal a distancia". Ocurre cuando dos o más partículas se vinculan de tal manera que sus estados cuánticos están intrínsecamente correlacionados, sin importar la distancia que las separe.[45] El estado del sistema compuesto no puede describirse como una simple combinación de los estados individuales de sus partes; debe describirse como un único estado cuántico global.[59] Matemáticamente, esto se expresa mediante el producto tensorial de los espacios de Hilbert de las partículas individuales. Un estado entrelazado es aquel que no puede ser factorizado en un simple producto tensorial de los estados de sus componentes.[59] Si se mide una propiedad de una partícula entrelazada (por ejemplo, su espín), el estado de la otra partícula se determina instantáneamente, sin importar cuán lejos esté.
- **Principio de Incertidumbre de Heisenberg:** Este principio establece un límite

fundamental a la precisión con la que se pueden conocer simultáneamente ciertos pares de propiedades físicas complementarias. El ejemplo más famoso es la posición (x) y el momento (p) de una partícula. Cuanto más precisamente se mide la posición, menos precisamente se puede conocer su momento, y viceversa.[61] Esta no es una limitación de los instrumentos de medida, sino una propiedad inherente de la naturaleza cuántica. Matemáticamente, surge de la no conmutatividad de los operadores cuánticos que representan estas propiedades. El conmutador de los operadores de posición y momento es
$[X,P]=i\hbar$, lo que conduce directamente a la famosa relación de incertidumbre: $\Delta x \Delta p \geq 2\hbar$.[33]

3.3 La Amenaza Cuántica: Cómo las Computadoras Cuánticas Rompen la Criptografía Clásica

Los principios abstractos y contra-intuitivos de la mecánica cuántica no son meras curiosidades filosóficas; son recursos computacionales concretos y explotables. La amenaza cuántica a la criptografía surge directamente de la capacidad de mapear un problema matemático clásicamente difícil (como la factorización) en un sistema físico cuyas leyes fundamentales de evolución (superposición e interferencia) son perfectamente adecuadas para resolverlo de manera eficiente.

- **El Poder del Qubit:** Una computadora clásica procesa información utilizando bits, que solo pueden estar en un estado de 0 o 1. Una computadora cuántica utiliza qubits. Gracias a la superposición, un qubit puede existir en un estado que es una combinación de $|0\rangle$ y $|1\rangle$: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$. Esto significa que un registro de N qubits puede representar los 2N estados posibles simultáneamente, proporcionando un espacio computacional masivamente paralelo.[54]
- Foco en el Algoritmo: El Algoritmo de Shor vs. RSA
  El algoritmo de Shor, desarrollado por Peter Shor en 1994, es el ejemplo más claro de la amenaza cuántica. No es un ataque de fuerza bruta, sino un elegante mapeo de un problema de teoría de números a un problema de física.
  - **El Problema:** La seguridad de RSA se basa en la dificultad clásica de encontrar los factores primos de un número grande N. Este problema de factorización está matemáticamente relacionado con encontrar el período de una función modular específica.
  - **La Solución Cuántica:** El algoritmo de Shor utiliza una computadora cuántica para encontrar eficientemente el período de la función $f(x)=a^x \pmod N$ para un número aleatorio a.[67]
  - **Mecanismo de Funcionamiento:**
    1. **Superposición como Recurso:** La computadora cuántica prepara un

registro de entrada en una superposición de todos los números posibles en un rango. Luego, calcula la función f(x) para todos estos valores simultáneamente en un solo paso computacional. El resultado es un estado cuántico masivo y entrelazado que contiene todos los pares de entrada y salida de la función.

2. **Interferencia como Recurso:** El paso crucial es la Transformada Cuántica de Fourier (QFT). La QFT actúa sobre el registro de entrada, provocando que las diferentes trayectorias computacionales interfieran entre sí. Las trayectorias que corresponden al período correcto de la función interfieren constructivamente, amplificando su probabilidad, mientras que las otras interfieren destructivamente y se anulan.[67]
3. **Medición:** Una medición final del registro de entrada revela, con alta probabilidad, un valor que está directamente relacionado con el período de la función.
4. **Post-procesamiento Clásico:** Con el período en mano, un algoritmo clásico puede calcular eficientemente los factores primos de N.

- **El Impacto:** Una computadora cuántica criptográficamente relevante podría ejecutar el algoritmo de Shor para factorizar una clave RSA de 2048 bits en cuestión de segundos o minutos, una tarea que para las supercomputadoras clásicas más potentes actuales llevaría milenios.[4] Esto hace que RSA y otros criptosistemas de clave pública basados en problemas similares queden completamente obsoletos.

Sección IV: Criptografía Cuántica: Seguridad a través de la Física

Mientras que la computación cuántica representa una amenaza existencial para la criptografía clásica, los mismos principios de la mecánica cuántica ofrecen un nuevo paradigma para la seguridad. La criptografía cuántica utiliza las propiedades de las partículas subatómicas para crear canales de comunicación teóricamente inexpugnables. Su aplicación más madura es la Distribución Cuántica de Claves (QKD), un método para compartir secretos que se basa en las leyes de la física en lugar de la dificultad computacional.

4.1 Distribución Cuántica de Claves (QKD): Un Intercambio Probablemente Seguro

- **Propósito Fundamental:** Es crucial entender que QKD no es un método para cifrar

mensajes. Su único propósito es permitir que dos partes, comúnmente llamadas Alice y Bob, generen y compartan una clave secreta perfectamente aleatoria. Esta clave se utiliza posteriormente para cifrar y descifrar mensajes utilizando un algoritmo de cifrado simétrico, como AES o, idealmente, una libreta de un solo uso (one-time pad), a través de un canal de comunicación clásico.[7]

- **Base de la Seguridad:** La seguridad de QKD se deriva de dos principios fundamentales de la mecánica cuántica, que hacen que la escucha clandestina (eavesdropping) sea detectable:
    - **El Teorema de No Clonación:** Es imposible crear una copia idéntica de un estado cuántico desconocido sin alterar el original. Esto impide que un espía, llamado Eve, intercepte un qubit, lo copie para su análisis posterior y envíe el original a Bob sin dejar rastro.[10]
    - **El Efecto Observador (Principio de Incertidumbre de Heisenberg):** Cualquier intento de medir una propiedad de un sistema cuántico lo perturba inevitablemente. Si Eve intercepta y mide un fotón enviado por Alice, alterará su estado cuántico. Esta alteración introducirá errores en las mediciones de Bob, que pueden ser detectados.[78]
- Protocolo Destacado: Un Recorrido por BB84
  El protocolo BB84, propuesto por Bennett y Brassard en 1984, es el arquetipo de los protocolos QKD. Su funcionamiento se desarrolla en varias etapas:
    1. **Configuración:** Alice y Bob se comunican a través de dos canales: un canal cuántico (por ejemplo, una fibra óptica) para transmitir fotones individuales, y un canal clásico autenticado (como una conexión a Internet) para discutir los resultados.[83]
    2. **Codificación (Alice):** Alice genera una cadena aleatoria de bits clásicos (0s y 1s). Para cada bit, elige al azar una de dos bases de polarización para codificarlo en un fotón: la base rectilínea (+) o la base diagonal (×). Por ejemplo, en la base +, un 0 puede ser un fotón polarizado horizontalmente (0∘) y un 1 uno polarizado verticalmente (90∘). En la base ×, un 0 puede ser 45∘ y un 1 ser 135∘ (o −45∘).[7]
    3. **Transmisión:** Alice envía la secuencia de fotones polarizados a Bob a través del canal cuántico.
    4. **Medición (Bob):** Para cada fotón que llega, Bob también elige al azar una de las dos bases (+ o ×) para medir su polarización.
    5. **Cribado (Discusión Pública):** A través del canal clásico, Alice y Bob anuncian públicamente la secuencia de bases que utilizaron para cada fotón, pero no los bits que enviaron o los resultados que midieron. Descartan todos los resultados de las mediciones en las que utilizaron bases diferentes. Estadísticamente, sus bases coincidirán en aproximadamente el 50% de los casos. Los bits restantes forman su "clave cribada" compartida.[84]
    6. **Verificación de Errores:** Alice y Bob sacrifican una porción aleatoria de su clave

cribada, comparando sus valores a través del canal clásico. Si un espía, Eve, hubiera intentado medir los fotones en tránsito, su elección aleatoria de base habría alterado inevitablemente algunos de los estados de los fotones, introduciendo errores en la clave de Bob incluso en los casos en que él y Alice usaron la misma base. Si la Tasa de Error de Bits Cuánticos (QBER) supera un umbral predefinido (por ejemplo, 25% en el protocolo BB84 ideal), asumen que la clave ha sido comprometida, la descartan por completo y reinician el proceso.[85]

7. **Destilación de la Clave:** Si la tasa de error es suficientemente baja, atribuyen los errores a imperfecciones del canal y del equipo. Luego aplican dos procedimientos clásicos: reconciliación de información (un protocolo de corrección de errores para asegurar que sus claves sean idénticas) y amplificación de la privacidad (un proceso para reducir cualquier información parcial que Eve pudiera haber obtenido a una cantidad arbitrariamente pequeña). El resultado es una clave final más corta, pero probadamente secreta y compartida.

4.2 La Frontera de la Implementación: De la Teoría a la Realidad

Existe una brecha significativa y a menudo subestimada entre la *seguridad teórica* de QKD, que es absoluta, y la *seguridad alcanzada* en un sistema práctico, que es condicional y altamente dependiente de la ingeniería. Esta brecha implica que QKD no elimina las suposiciones de confianza, sino que las desplaza de la dureza computacional a la integridad física y el rendimiento ideal del hardware.

- **Análisis de los Desafíos Prácticos:** A pesar de su elegancia teórica, la implementación de QKD en el mundo real se enfrenta a obstáculos considerables:
    - **Distancia y Atenuación:** Los fotones se pierden o son absorbidos en las fibras ópticas, un fenómeno conocido como atenuación. Esto limita el alcance práctico de los enlaces QKD terrestres a unos pocos cientos de kilómetros. Para una red global se necesitarían repetidores cuánticos, una tecnología que aún está en fase de investigación y desarrollo.[89]
    - **Imperfecciones del Hardware:** La teoría de QKD asume fuentes de fotones únicos y detectores 100% eficientes, ninguno de los cuales existe en la práctica. Los sistemas reales utilizan láseres atenuados que a veces emiten pulsos con múltiples fotones, lo que los hace vulnerables a ataques de división de número de fotones (PNS), donde Eve puede separar un fotón para medirlo sin perturbar el resto del pulso.[89] Las ineficiencias y los tiempos de respuesta de los detectores también pueden ser explotados en ataques de canal lateral. La Agencia de Seguridad Nacional de EE. UU. (NSA) afirma explícitamente que la seguridad es "altamente dependiente de la implementación en lugar de estar asegurada por

las leyes de la física".[92]

- **Requisito de Autenticación:** QKD por sí mismo no proporciona autenticación. Para evitar un ataque de "hombre en el medio" (man-in-the-middle), donde Eve se hace pasar por Bob ante Alice y por Alice ante Bob, el canal clásico utilizado para el cribado y la verificación de errores debe ser autenticado. Esto requiere un secreto precompartido o el uso de criptografía de clave pública clásica (que debe ser post-cuántica para ser segura a largo plazo).[89]
- **Infraestructura y Costo:** QKD requiere hardware especializado y costoso (fuentes de fotones, detectores de fotones únicos) y, a menudo, fibras ópticas dedicadas ("fibra oscura"), lo que dificulta y encarece su integración en las redes de comunicación existentes.[92]
- **Denegación de Servicio (DoS):** La misma sensibilidad que permite a QKD detectar escuchas también lo hace vulnerable a ataques de denegación de servicio. Un atacante puede simplemente introducir ruido en el canal cuántico para aumentar la tasa de error por encima del umbral de seguridad, obligando a Alice y Bob a abortar continuamente el proceso de generación de claves.[92]

- Estado Global: Un Vistazo a los Bancos de Pruebas y Redes QKD
  A pesar de estos desafíos, la viabilidad de QKD se ha demostrado en numerosas redes y bancos de prueba en todo el mundo, principalmente en entornos metropolitanos. Ejemplos notables incluyen la red SECOQC en Viena, redes en Madrid, Berlín y Poznan, el enlace satelital Micius de China que conecta Beijing y Viena, y redes de investigación en EE. UU. como la Chicago Quantum Exchange.93 Estas implementaciones suelen basarse en una arquitectura de "nodos de confianza", donde los repetidores intermedios son puntos seguros que descifran y re-cifran la clave, lo que significa que la seguridad de extremo a extremo depende de la seguridad física de cada nodo en la cadena.

Sección V: Criptografía Post-Cuántica (PQC): Construyendo un Futuro Resistente a lo Cuántico

En paralelo al desarrollo de la criptografía basada en la física, la comunidad criptográfica global ha estado trabajando en una solución alternativa y más pragmática a la amenaza cuántica: la criptografía post-cuántica (PQC). Este enfoque busca desarrollar nuevos algoritmos de criptografía clásica que sean seguros contra ataques tanto de computadoras clásicas como cuánticas.

5.1 El Paradigma PQC: Algoritmos Clásicos para un Mundo Cuántico

- **Definición:** La criptografía post-cuántica (también llamada criptografía resistente a lo cuántico) consiste en algoritmos diseñados para ejecutarse en computadoras clásicas convencionales, pero cuya seguridad se basa en problemas matemáticos que se cree que son difíciles de resolver tanto para las computadoras clásicas como para las cuánticas.[98]
- **Distinción con QKD:** A diferencia de QKD, que es un sistema de hardware para la distribución de claves, PQC es una solución basada en software. Esto significa que los algoritmos PQC pueden integrarse en los protocolos y la infraestructura de red existentes (como TLS, VPNs, etc.) con actualizaciones de software, sin necesidad de hardware especializado como fuentes de fotones o fibras ópticas dedicadas.[92]

5.2 El Proceso de Estandarización del NIST: Forjando Nuevos Estándares

El proceso de estandarización de PQC del NIST representa un giro estratégico global hacia la diversidad criptográfica como principio fundamental de seguridad. La selección de múltiples familias algorítmicas es una estrategia deliberada de gestión de cartera, diseñada para cubrir el riesgo de un futuro avance criptoanalítico que pudiera comprometer toda una clase de problemas matemáticos. Mientras que la infraestructura de clave pública actual es en gran medida un monocultivo que depende de la factorización y los logaritmos discretos (ambos vulnerables al algoritmo de Shor), el enfoque del NIST ha sido diversificar. Al estandarizar algoritmos de familias matemáticas distintas (redes, hashes, códigos), se crea un ecosistema resiliente. Si se descubre un ataque contra los problemas basados en redes, la existencia de alternativas estandarizadas y examinadas de otras familias, como las basadas en hashes, permitiría una migración rápida y segura. Esta diversificación, combinada con el principio arquitectónico de la agilidad criptográfica, marca un cambio fundamental: pasar de confiar en la dureza percibida de un único problema a construir un ecosistema que pueda soportar el fallo de cualquiera de sus componentes.

- **Motivación:** Ante la inminente amenaza que representan las computadoras cuánticas, el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. inició en 2016 un proceso público y global para solicitar, evaluar y estandarizar una nueva suite de algoritmos criptográficos de clave pública resistentes a los cuánticos.[99]
- **Proceso:** El proceso, que duró varios años, consistió en múltiples rondas de evaluación. Criptógrafos de todo el mundo presentaron 82 algoritmos candidatos, que fueron sometidos a un intenso escrutinio público y criptoanálisis por parte de la comunidad académica e industrial para identificar las propuestas más seguras y eficientes.[100]
- **Estándares Finalizados (a partir de 2024):** En agosto de 2024, el NIST anunció la publicación de los primeros tres estándares PQC finalizados:
    - **ML-KEM (CRYSTALS-Kyber):** Publicado como FIPS 203, es el estándar principal

para los Mecanismos de Encapsulación de Claves (KEM), utilizados para el establecimiento seguro de claves compartidas. Es un algoritmo basado en redes.[105]
    - **ML-DSA (CRYSTALS-Dilithium):** Publicado como FIPS 204, es el estándar principal para firmas digitales. También es un algoritmo basado en redes.[105]
    - **SLH-DSA (SPHINCS+):** Publicado como FIPS 205, es un estándar secundario para firmas digitales. Se basa en funciones hash y se estandarizó para proporcionar diversidad algorítmica como respaldo en caso de que se descubra una vulnerabilidad en los esquemas basados en redes.[105]
- **Esfuerzos en Curso:** Se espera un cuarto estándar basado en el algoritmo FALCON para finales de 2024. Además, el NIST continúa evaluando candidatos adicionales, incluyendo algoritmos basados en códigos, para futuras estandarizaciones y así aumentar la diversidad del conjunto de herramientas PQC.[104]

5.3 Un Vistazo a los Enfoques PQC

- **Criptografía Basada en Redes (Lattices):**
    - **Problema Difícil:** La seguridad se basa en la dificultad de resolver problemas en retículos de alta dimensión, como el Problema del Vector Más Corto (SVP) o el Aprendizaje con Errores (LWE). Un retículo es un conjunto de puntos en un espacio n-dimensional que forman una cuadrícula regular.[98]
    - **Estado:** Es el enfoque más prometedor y el que ha recibido más investigación. Los estándares primarios del NIST, ML-KEM y ML-DSA, son ambos esquemas basados en redes.[106]
    - **Características:** Ofrecen un buen equilibrio entre seguridad, rendimiento y tamaño de clave, aunque sus claves y firmas son generalmente más grandes que las de la criptografía de curva elíptica.[112]
- **Criptografía Basada en Códigos:**
    - **Problema Difícil:** La seguridad se basa en la dificultad de decodificar un código lineal general de corrección de errores, un problema que es NP-duro.[113]
    - **Ejemplo:** El criptosistema de McEliece, propuesto en 1978, es uno de los criptosistemas de clave pública más antiguos y aún no ha sido vulnerado. Una variante, Classic McEliece, es finalista en el proceso del NIST para una futura estandarización.[114]
    - **Características:** Goza de una gran confianza en su seguridad, pero su principal inconveniente son los tamaños de clave pública extremadamente grandes, que pueden ser del orden de megabytes.
- **Criptografía Basada en Hashes:**
    - **Problema Difícil:** La seguridad se deriva directamente de las propiedades de

resistencia a colisiones y preimágenes de las funciones hash criptográficas estándar, como SHA-256.[98]

- **Ejemplo:** SPHINCS+ (ahora estandarizado como SLH-DSA) es un esquema de firma digital sin estado. Los esquemas anteriores, como las firmas de Merkle, eran "con estado", lo que significaba que una clave privada solo podía usarse para firmar un número limitado de mensajes.[98]
- **Características:** La seguridad está muy bien comprendida, pero las firmas tienden a ser más grandes y el proceso de firma y verificación es más lento en comparación con los esquemas basados en redes.

5.4 El Camino a Seguir: Migración Estratégica

La transición de la criptografía actual a PQC es una tarea monumental que afectará a casi todos los sistemas digitales.

- **Agilidad Criptográfica (Crypto-Agility):** Es la capacidad de una infraestructura de TI para cambiar o actualizar de manera rápida y eficiente los algoritmos criptográficos que utiliza. Este es un imperativo estratégico clave para la migración a PQC. Permite a las organizaciones adaptarse a medida que se publican nuevos estándares, se descubren vulnerabilidades o cambian los requisitos de rendimiento, sin tener que rediseñar sistemas enteros.[116]
- **Enfoque Híbrido:** Durante el período de transición, una estrategia recomendada es el uso de un enfoque híbrido. En este modo, la comunicación se asegura utilizando tanto un algoritmo clásico (como ECC) como un algoritmo PQC (como Kyber). Por ejemplo, para establecer una clave de sesión, se generarían dos secretos compartidos, uno con cada algoritmo, y luego se combinarían para derivar la clave final. Este enfoque garantiza que la comunicación permanezca segura incluso si uno de los algoritmos se rompe, proporcionando protección tanto contra atacantes clásicos como cuánticos.[116]
- **Cronograma de Migración:** La transición completa es un esfuerzo a largo plazo. Organismos gubernamentales como el NIST en EE. UU. y el NCSC en el Reino Unido han establecido plazos que apuntan a una migración completa de los sistemas críticos para aproximadamente el año 2035.[108] La urgencia se ve acentuada por la amenaza de "cosechar ahora, descifrar después", donde los adversarios pueden estar almacenando datos cifrados hoy con la intención de descifrarlos en el futuro una vez que dispongan de una computadora cuántica.

Sección VI: Conclusión: Navegando por el Nuevo Paisaje Criptográfico

6.1 Síntesis de Paradigmas

Este informe ha trazado un recorrido desde los fundamentos matemáticos de la criptografía clásica hasta la inminente revolución impulsada por la física cuántica. Hemos visto cómo la seguridad en el mundo digital ha evolucionado de depender de la dificultad computacional de problemas como la factorización (RSA) a enfrentarse a una amenaza existencial por parte de computadoras cuánticas que pueden resolver dichos problemas de manera eficiente (algoritmo de Shor).

En respuesta a esta amenaza, han surgido dos caminos distintos pero complementarios. El primero, la criptografía cuántica, en particular la Distribución Cuántica de Claves (QKD), ofrece una seguridad basada en las leyes fundamentales de la física, prometiendo un intercambio de claves teóricamente inexpugnable. Sin embargo, su implementación práctica está limitada por desafíos de hardware, distancia e infraestructura. El segundo camino, la criptografía post-cuántica (PQC), representa un enfoque pragmático: el desarrollo de nuevos algoritmos clásicos basados en problemas matemáticos que se cree son resistentes incluso a los ataques cuánticos. El proceso de estandarización del NIST ha culminado en un primer conjunto de herramientas PQC listas para su despliegue.

6.2 La Amenaza Evolutiva y la Urgencia de la Transición

La pregunta ya no es si las organizaciones deben migrar a una criptografía resistente a los cuánticos, sino cuándo y cómo. Aunque el cronograma para la llegada de una computadora cuántica criptográficamente relevante (CRQC) sigue siendo incierto, el consenso de expertos lo sitúa dentro de los próximos 10 a 20 años, con organismos gubernamentales estableciendo plazos de migración en torno a 2035.[108]

La urgencia de esta transición se ve magnificada por la amenaza de "cosechar ahora, descifrar después" (*harvest now, decrypt later*). Los adversarios pueden interceptar y almacenar datos cifrados hoy con los algoritmos actuales y simplemente esperar a que una CRQC esté disponible para descifrarlos. Esto significa que cualquier dato que deba permanecer secreto durante la próxima década o más ya es vulnerable.

La estrategia a seguir debe ser proactiva y ágil. La adopción de la agilidad criptográfica como principio de diseño y la implementación de un enfoque híbrido son pasos intermedios cruciales que permiten a las organizaciones comenzar la transición, mitigar los riesgos a corto plazo y prepararse para un futuro totalmente post-cuántico.

A continuación, se presenta una tabla que resume y compara las características fundamentales de los tres paradigmas criptográficos discutidos.

Tabla 1: Un Análisis Comparativo de los Paradigmas Criptográficos

Característica	Criptografía Clásica (ej. RSA/ECC)	Distribución Cuántica de Claves (QKD)	Criptografía Post-Cuántica (PQC)
Base de la Seguridad	Dificultad Computacional (Problemas Matemáticos)	Leyes de la Física Cuántica	Dificultad Computacional (Nuevos Problemas Matemáticos)
Función Principal	Cifrado, Firmas Digitales, Intercambio de Claves	Solo Intercambio Seguro de Claves	Cifrado, Firmas Digitales, Intercambio de Claves
Gestión de Claves	Infraestructura de Clave Pública (PKI)	Canal Cuántico + Canal Clásico Autenticado	Infraestructura de Clave Pública (PKI)
Vulnerabilidad Principal	Algoritmos Cuánticos (ej. Shor)	Fallos de Implementación, Canales Laterales, DoS	Futuros Avances Matemáticos/Cuánticos
Infraestructura	Software y Redes Existentes	Hardware Especializado (Fotónica), Fibra Óptica	Software y Redes Existentes (con actualizaciones)
Nivel de Madurez	Maduro, Ampliamente Desplegado	Emergente, Despliegues de Nicho	Recién Estandarizado, Adopción Temprana

Fuentes citadas

1. cryptography - Glossary | CSRC - NIST Computer Security Resource Center, acceso: agosto 12, 2025, https://csrc.nist.gov/glossary/term/cryptography
2. What is Cryptography? Definition of Data Encryption Methods - AWS, acceso: agosto 12, 2025, https://aws.amazon.com/what-is/cryptography/
3. What Is Cryptography In Security? | Types Of Cryptography - Encryption Consulting, acceso: agosto 12, 2025, https://www.encryptionconsulting.com/education-center/what-is-cryptography/
4. Cryptography - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/Cryptography
5. Goals of Cryptography - UMSL, acceso: agosto 12, 2025, https://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/Cryptography%20and%20goals.html
6. Symmetric vs Asymmetric Encryption: What's the difference? - Mailfence Blog, acceso: agosto 12, 2025, https://blog.mailfence.com/symmetric-vs-asymmetric-encryption/
7. Quantum cryptography - CS Stanford, acceso: agosto 12, 2025, https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-

05/cryptography/quantum.html
8. What is RSA? How does an RSA work? - Encryption Consulting, acceso: agosto 12, 2025, https://www.encryptionconsulting.com/education-center/what-is-rsa/
9. What is Quantum Cryptography? - Ironscales, acceso: agosto 12, 2025, https://ironscales.com/glossary/quantum-cryptography
10. What is Quantum Cryptography? - AZoQuantum, acceso: agosto 12, 2025, https://www.azoquantum.com/Article.aspx?ArticleID=117
11. deviceauthority.com, acceso: agosto 12, 2025, https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/#:~:text=Symmetric%20encryption%20uses%20the%20same%20key%20for%20encryption%20and%20decryption,more%20secure%20for%20certain%20applications.
12. Symmetric and asymmetric encryption explained: RSA vs. AES - Prey Project, acceso: agosto 12, 2025, https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes
13. Symmetric Encryption vs Asymmetric Encryption: How it Works and Why it's Used, acceso: agosto 12, 2025, https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/
14. Symmetric vs. Asymmetric Encryption: What's the Difference? - Trenton Systems, acceso: agosto 12, 2025, https://www.trentonsystems.com/en-us/resource-hub/blog/symmetric-vs-asymmetric-encryption
15. Symmetric and Asymmetric Key Encryption – Explained in Plain English - freeCodeCamp, acceso: agosto 12, 2025, https://www.freecodecamp.org/news/encryption-explained-in-plain-english/
16. AES Encryption: How it works, Benefits, and Use Cases - Splashtop, acceso: agosto 12, 2025, https://www.splashtop.com/blog/aes-encryption
17. Advanced Encryption Standard - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
18. What is AES Encryption and How Does It Work? - Cybernews, acceso: agosto 12, 2025, https://cybernews.com/resources/what-is-aes-encryption/
19. Just a quick question for trying to understand AES : r/cryptography - Reddit, acceso: agosto 12, 2025, https://www.reddit.com/r/cryptography/comments/u62jaj/just_a_quick_question_for_trying_to_understand_aes/
20. RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained | Splunk, acceso: agosto 12, 2025, https://www.splunk.com/en_us/blog/learn/rsa-algorithm-cryptography.html
21. Understanding RSA Asymmetric Encryption: How It Works - SecureW2, acceso: agosto 12, 2025, https://www.securew2.com/blog/what-is-rsa-asymmetric-encryption
22. What Is Symmetric Encryption? - IBM, acceso: agosto 12, 2025, https://www.ibm.com/think/topics/symmetric-encryption
23. What is Asymmetric Encryption? - IBM, acceso: agosto 12, 2025,

https://www.ibm.com/think/topics/asymmetric-encryption
24. www.movable-type.co.uk, acceso: agosto 12, 2025, https://www.movable-type.co.uk/scripts/sha256.html#:~:text=A%20cryptographic%20hash%20(sometimes%20called,byte)%20signature%20for%20a%20text.
25. SHA-256 Cryptographic Hash Algorithm implemented in JavaScript | Movable Type Scripts, acceso: agosto 12, 2025, https://www.movable-type.co.uk/scripts/sha256.html
26. What Is SHA-256? | Boot.dev, acceso: agosto 12, 2025, https://blog.boot.dev/cryptography/how-sha-2-works-step-by-step-sha-256/
27. What is Secure Hash Algorithm 256-bit (SHA-256)? - Securiti.ai, acceso: agosto 12, 2025, https://securiti.ai/glossary/secure-hash-algorithm-sha-256-bit/
28. Física del siglo XX: Cuántica | EL GATO DE SCHRÖDINGER. Blog de física y química. - Gobierno de Canarias, acceso: agosto 5, 2025, https://www3.gobiernodecanarias.org/medusa/ecoblog/mramrodp/?p=2436
29. Radiación de cuerpo negro y catástrofe ultravioleta | Los Mundos de ..., acceso: agosto 5, 2025, https://losmundosdebrana.com/2014/03/10/radiacion-de-cuerpo-negro-y-catastrofe-ultravioleta/
30. fisicatabu.com, acceso: agosto 5, 2025, https://fisicatabu.com/tema-30-teoria-cuantica-problemas-precursores-limites-de-la-fisica-clasica-para-resolverlos-fenomenos-que-corroboran-la-teoria-cuantica/#:~:text=La%20teor%C3%ADa%20cl%C3%A1sica%20fallaba%20al,onda%20peque%C3%B1as%20(altas%20frecuencias).&text=Este%20problema%20lo%20solucionar%C3%ADa%20el,dando%20inicio%20a%20la%20cu%C3%A1ntica.
31. Teoría cuántica. Problemas precursores. Límites de la física clásica ..., acceso: agosto 5, 2025, https://fisicatabu.com/tema-30-teoria-cuantica-problemas-precursores-limites-de-la-fisica-clasica-para-resolverlos-fenomenos-que-corroboran-la-teoria-cuantica/
32. RADIACIÓN DE CUERPO NEGRO, CATÁSTROFE ULTRAVIOLETA E HIPÓTESIS DE PLANCK - YouTube, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=Uk4fq07Fzxg
33. UnaintroducciónalaMecánicaCuántica Prof.Dr.Renato ..., acceso: julio 18, 2025, https://renato.ryn-fismat.es/papers/cuantica.pdf
34. Introducción al formalismo de la mecánica cuántica no relativista, acceso: julio 18, 2025, https://repositorio.unal.edu.co/bitstream/handle/unal/84250/35.%20Introducci%C2%A2n%20al%20formalismo%20de%20la%20mec%E2%80%A0nica%20cu%E2%80%A0ntica%20no%20relativista.pdf?sequence=2&isAllowed=y
35. Qué es el efecto fotoeléctrico resumen - Resueltoos.com, acceso: agosto 5, 2025, https://www.resueltoos.com/blog/fisica-y-quimica/efecto-fotoelectrico
36. Efecto fotoeléctrico (artículo) | Khan Academy, acceso: agosto 5, 2025, https://es.khanacademy.org/science/ap-chemistry/electronic-structure-of-atoms-ap/bohr-model-hydrogen-ap/a/photoelectric-effect

37. 6.2 Efecto fotoeléctrico - Física universitaria volumen 3 | OpenStax, acceso: agosto 5, 2025, https://openstax.org/books/f%C3%ADsica-universitaria-volumen-3/pages/6-2-efecto-fotoelectrico
38. Efecto fotoeléctrico - Wikipedia, la enciclopedia libre, acceso: agosto 5, 2025, https://es.wikipedia.org/wiki/Efecto_fotoel%C3%A9ctrico
39. EFECTO FOTOELÉCTRICO: Explicación Simple y Clara - YouTube, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=vdbJfP7WtZk
40. Mecánica cuántica - Wikipedia, la enciclopedia libre, acceso: agosto 5, 2025, https://es.wikipedia.org/wiki/Mec%C3%A1nica_cu%C3%A1ntica
41. ¿Qué es el efecto fotoeléctrico? | Explora - Univision, acceso: agosto 5, 2025, https://www.univision.com/explora/que-es-el-efecto-fotoelectrico
42. ¿Sabes lo que es el efecto fotoeléctrico? - YouTube, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=wj9FRoiRHYc
43. El efecto fotoeléctrico, ¿En qué consiste? | Blog de Fundeen, acceso: agosto 5, 2025, https://www.fundeen.com/blog-energias-renovables/el-efecto-fotoelectrico-en-que-consiste
44. La explicación de Einstein del efecto fotoeléctrico: un análisis histórico-epistemológico, acceso: agosto 5, 2025, https://www.researchgate.net/publication/262498776_La_explicacion_de_Einstein_del_efecto_fotoelectrico_un_analisis_historico-epistemologico
45. Física cuántica para principiantes: guía simple y clara - Ambientum, acceso: agosto 5, 2025, https://www.ambientum.com/ambientum/ciencia/fisica-cuantica-para-principiantes-guia-simple-y-clara.asp
46. Física Cuántica desde cero para principiantes (en menos de 15 minutos) - La doble rendija, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=x_59G83J0Ws
47. Física Cuántica desde cero para principiantes (en menos de 15 minutos) - La doble rendija, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=x_59G83J0Ws&pp=0gcJCfwAo7VqN5tD
48. La Dualidad Onda-Partícula: El Misterio de De Broglie (Física Cuántica) - YouTube, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=Cxa2ljy_Zoo
49. Física 7.03 Dualidad onda-partícula. Hipótesis de de Broglie. Explicación-demostración muy sencilla. - YouTube, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=TbWa3KSfQWA
50. Dualidad onda corpúsculo - Wikipedia, la enciclopedia libre, acceso: agosto 5, 2025, https://es.wikipedia.org/wiki/Dualidad_onda_corp%C3%BAsculo
51. Resumen de La Mecánica Cuántica Escuela PCE, acceso: agosto 5, 2025, https://escuelapce.com/resumen-de-la-mecanica-cuantica/
52. introducción al concepto de superposición en mecánica cuántica mediante los fundamentos de la computación - Universidad Pedagógica Nacional, acceso: julio 18, 2025, http://repository.pedagogica.edu.co/bitstream/handle/20.500.12209/19366/introduccion%20al%20concepto%20de%20superposicion.pdf?sequence=4&isAllowe

d=y
53. Las matemáticas (para todos) detrás de la superposición cuántica ..., acceso: julio 18, 2025, https://www.muyinteresante.com/ciencia/matematicas-superposicion-cuantica-gato.html
54. ¿En qué consiste la computación cuántica? - AWS, acceso: julio 18, 2025, https://aws.amazon.com/es/what-is/quantum-computing/
55. es.wikipedia.org, acceso: agosto 5, 2025, https://es.wikipedia.org/wiki/Entrelazamiento_cu%C3%A1ntico#:~:text=El%20entrelazamiento%20es%20un%20fen%C3%B3meno,los%20objetos%20est%C3%A9n%20separados%20espacialmente.
56. ¿Qué es el entrelazamiento cuántico? - YouTube, acceso: agosto 5, 2025, https://m.youtube.com/watch?v=7KKYcbwJjeQ
57. ¿Qué es el entrelazamiento cuántico y por qué es importante? - YouTube, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=bUM8UN_KhE4
58. Cómo se midió por primera vez el entrelazamiento cuántico - Elementos - Publicación, acceso: agosto 5, 2025, https://elementos.buap.mx/post.php?id=1061
59. Más entrelazados que nunca - Bosoneando, acceso: julio 18, 2025, http://bosoneando.blogspot.com/2015/01/mas-entrelazados-que-nunca.html
60. ¿Se pueden separar los estados entrelazados cuánticos en sus superposiciones con respecto al producto tensorial? - Academia EITCA, acceso: julio 18, 2025, https://es.eitca.org/informaci%C3%B3n-cu%C3%A1ntica/eitc-qi-qif-informaci%C3%B3n-cu%C3%A1ntica-fundamentos/entrelazamiento-cu%C3%A1ntico/enredo/%C2%BFSe-pueden-separar-los-estados-entrelazados-cu%C3%A1nticos-en-sus-superposiciones-con-respecto-al-producto-tensorial%3F/
61. Principio de Incertidumbre de Heisenberg - Hiberus Tecnología, acceso: agosto 5, 2025, https://www.hiberus.com/crecemos-contigo/principio-de-incertidumbre-de-heisenberg/
62. 7.2 El principio de incertidumbre de Heisenberg - Física universitaria volumen 3 | OpenStax, acceso: agosto 5, 2025, https://openstax.org/books/f%C3%ADsica-universitaria-volumen-3/pages/7-2-el-principio-de-incertidumbre-de-heisenberg
63. TODAY YOU WILL UNDERSTAND THE UNCERTAINTY PRINCIPLE - YouTube, acceso: agosto 5, 2025, https://www.youtube.com/watch?v=JnEAMYltzi0&pp=0gcJCfwAo7VqN5tD
64. El principio de indeterminación – Física cuántica en la red, acceso: julio 18, 2025, https://www.fisicacuantica.es/el-principio-de-indeterminacion/
65. Computación Cuántica Básica con Álgebra Lineal - Departamento de Matemáticas | Facultad de Ciencias UAM, acceso: julio 18, 2025, http://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_claudia_mielgo.pdf
66. Conceptos Matemáticos Básicos de Computación Cuántica - DocIRS, acceso:

julio 18, 2025, https://www.docirs.cl/math_computacion_cuantica.asp
67. Implementation and Analysis of Shor's Algorithm to Break RSA Cryptosystem Security, acceso: agosto 12, 2025, https://www.researchgate.net/publication/377245624_Implementation_and_Analysis_of_Shor's_Algorithm_to_Break_RSA_Cryptosystem_Security
68. Using Shor's Algorithm to Break RSA Encryption - PhysLab, acceso: agosto 12, 2025, https://physlab.org/wp-content/uploads/2023/04/Shor_23100113-1.pdf
69. Shor's algorithm - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/Shor%27s_algorithm
70. Quantum Cryptography - Shor's Algorithm Explained - Classiq, acceso: agosto 12, 2025, https://www.classiq.io/insights/shors-algorithm-explained
71. www.qutube.nl, acceso: agosto 12, 2025, https://www.qutube.nl/quantum-algorithms/shors-algorithm#:~:text=In%20general%20terms%2C%20Shor's%20algorithm,of%20two%20large%20prime%20numbers.
72. Quantum key distribution - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/Quantum_key_distribution
73. The No-cloning Theorem and its Implications in Quantum Cryptography, acceso: agosto 12, 2025, https://www.sas.rochester.edu/pas/undergraduate/kapitza_paper_nocloning_s2022.pdf
74. Fundamental limits on quantum cloning from the no-signaling principle | Phys. Rev. A, acceso: agosto 12, 2025, https://link.aps.org/doi/10.1103/PhysRevA.109.022221
75. What is No-Cloning Theorem - QuEra Computing, acceso: agosto 12, 2025, https://www.quera.com/glossary/no-cloning-theorem
76. No-cloning theorem - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/No-cloning_theorem
77. Basic Quantum Computing — No Cloning Theorem | by Charlie Thomas | Medium, acceso: agosto 12, 2025, https://medium.com/@charlie.thomas_94667/basic-quantum-computing-no-cloning-theorem-b5c0d17000ed
78. Cryptography in the Quantum Age | NIST, acceso: agosto 12, 2025, https://www.nist.gov/physics/introduction-new-quantum-revolution/cryptography-quantum-age
79. www.nist.gov, acceso: agosto 12, 2025, https://www.nist.gov/physics/introduction-new-quantum-revolution/cryptography-quantum-age#:~:text=The%20uncertainty%20principle%20indicates%20that,way%20that%20can%20be%20detected.
80. How does the Heisenberg uncertainty principle contribute to the security of Quantum Key Distribution (QKD)? - EITCA Academy, acceso: agosto 12, 2025, https://eitca.org/cybersecurity/eitc-is-qcf-quantum-cryptography-fundamentals/practical-quantum-key-distribution/quantum-hacking-part-

1/examination-review-quantum-hacking-part-1/how-does-the-heisenberg-uncertainty-principle-contribute-to-the-security-of-quantum-key-distribution-qkd/
81. Quantum Fundamentals – The Uncertainty Principle - AZoQuantum, acceso: agosto 12, 2025, https://www.azoquantum.com/Article.aspx?ArticleID=616
82. What Is the Uncertainty Principle and Why Is It Important? - Caltech Science Exchange, acceso: agosto 12, 2025, https://scienceexchange.caltech.edu/topics/quantum-science-explained/uncertainty-principle
83. BB84 - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/BB84
84. Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol - arXiv, acceso: agosto 12, 2025, https://arxiv.org/html/2312.05609v1
85. Quantum Key Distribution (QKD) and the BB84 Protocol, acceso: agosto 12, 2025, https://postquantum.com/post-quantum/qkd-bb84/
86. Quantum Key Distribution (QKD) - QuIC Lab, acceso: agosto 12, 2025, https://www.rri.res.in/quic/qcommconcepts.php
87. Lecture 12: Quantum key distribution. Secret key. BB84, E91 and B92 protocols. Continuous-variable protocols. 1. Secret, acceso: agosto 12, 2025, https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12.pdf
88. An Overview of Quantum Key Distribution Protocols and Experimental Implementations, acceso: agosto 12, 2025, https://wp.optics.arizona.edu/opti646/wp-content/uploads/sites/55/2022/12/Zhai_Term_Paper.pdf
89. Challenges of implementing quantum key distribution - Hlk-ip.com, acceso: agosto 12, 2025, https://www.hlk-ip.com/news-and-insights/challenges-of-implementing-quantum-key-distribution/
90. Large scale quantum key distribution: challenges and solutions [Invited] - Optics Express, acceso: agosto 12, 2025, https://opg.optica.org/abstract.cfm?uri=oe-26-18-24260
91. Quantum cryptography - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/Quantum_cryptography
92. Quantum Key Distribution (QKD) and Quantum Cryptography QC - National Security Agency, acceso: agosto 12, 2025, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
93. Quantum Key Distribution (QKD) 101: A Guide for Cybersecurity Professionals, acceso: agosto 12, 2025, https://postquantum.com/post-quantum/quantum-key-distribution-qkd-cyber/
94. Why Quantum Key Distribution (QKD) is impractical - Cryptography Stack Exchange, acceso: agosto 12, 2025, https://crypto.stackexchange.com/questions/93830/why-quantum-key-distribution-qkd-is-impractical

95. Quantum Key Distribution | QKD | Quantum Cryptography - ID Quantique, acceso: agosto 12, 2025, https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/
96. 1 Introduction - arXiv, acceso: agosto 12, 2025, https://arxiv.org/html/2311.08038v3
97. Quantum Key Distribution in-field implementations - JRC Publications Repository, acceso: agosto 12, 2025, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118150/quantum_communication_state-of-the-art__review_4.0_final.pdf
98. Post-quantum cryptography - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/Post-quantum_cryptography
99. Post-Quantum Cryptography | NIST, acceso: agosto 12, 2025, https://www.nist.gov/programs-projects/post-quantum-cryptography
100. What Is Post-Quantum Cryptography? | NIST, acceso: agosto 12, 2025, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography
101. What is Post-Quantum Cryptography (PQC)? - Palo Alto Networks, acceso: agosto 12, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc
102. Post-Quantum Cryptography, Explained - Booz Allen, acceso: agosto 12, 2025, https://www.boozallen.com/insights/ai-research/post-quantum-cryptography-explained.html
103. An In-Depth Look at NIST's Post-Quantum Algorithms - EntropiQ, acceso: agosto 12, 2025, https://entropiq.com/nist-post-quantum-algorithms/
104. NIST Post-Quantum Cryptography Standardization - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization
105. Post-Quantum Cryptography | CSRC - NIST Computer Security Resource Center, acceso: agosto 12, 2025, https://csrc.nist.gov/projects/post-quantum-cryptography
106. NIST Releases First 3 Finalized Post-Quantum Encryption Standards, acceso: agosto 12, 2025, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
107. What is Post-Quantum Cryptography (PQC)? - Lattice Semiconductor, acceso: agosto 12, 2025, https://www.latticesemi.com/what-is-post-quantum-cryptography
108. Timelines for migration to post-quantum cryptography - NCSC.GOV.UK, acceso: agosto 12, 2025, https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
109. Post-quantum cryptography: Lattice-based cryptography - Red Hat, acceso: agosto 12, 2025, https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography
110. Lattice-based cryptography - Wikipedia, acceso: agosto 12, 2025, https://en.wikipedia.org/wiki/Lattice-based_cryptography

111. NSAs Cybersecurity Perspective on Post Quantum Cryptography Algorithms, acceso: agosto 12, 2025, https://www.nsa.gov/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/
112. Prepping for post-quantum: a beginner's guide to lattice cryptography - The Cloudflare Blog, acceso: agosto 12, 2025, https://blog.cloudflare.com/lattice-crypto-primer/
113. [2505.08791] Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems - arXiv, acceso: agosto 12, 2025, https://arxiv.org/abs/2505.08791
114. What is Code-based Cryptography? - Utimaco, acceso: agosto 12, 2025, https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-code-based-cryptography
115. Post-quantum cryptography: Code-based cryptography - Red Hat, acceso: agosto 12, 2025, https://www.redhat.com/en/blog/post-quantum-cryptography-code-based-cryptography
116. Uncovering the advantages of hybridization and crypto-agility in quantum security - Eviden, acceso: agosto 12, 2025, https://eviden.com/publications/digital-security-magazine/cybersecurity-predictions-2025/hybridization-crypto-agility-quantum-security/
117. Post-Quantum Crypto Agility - Thales CPL, acceso: agosto 12, 2025, https://cpl.thalesgroup.com/encryption/post-quantum-crypto-agility
118. Cryptographic Agility for Control over Hybrid Post-Quantum TLS - QuSecure, acceso: agosto 12, 2025, https://www.qusecure.com/cryptographic-agility-for-control-over-hybrid-post-quantum-tls/
119. Embracing Crypto-agility for Quantum-safe Business - Tata Consultancy Services, acceso: agosto 12, 2025, https://www.tcs.com/what-we-do/services/cybersecurity/white-paper/crypto-agility-quantum-computing-safety
120. NIST Outlines Strategies for Crypto Agility as PQC Migration Stalls, Available for Public Comment - The Quantum Insider, acceso: agosto 12, 2025, https://thequantuminsider.com/2025/03/07/nist-outlines-strategies-for-crypto-agility-as-pqc-migration-stalls-available-for-public-comment/
121. Migration to Post-Quantum Cryptography - NCCoE, acceso: agosto 12, 2025, https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
122. NIST recommends timelines for transitioning cryptographic algorithms | PQShield, acceso: agosto 12, 2025, https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/
123. NIST Issues Draft Post Quantum Cryptography Transition Strategy and Timeline - HPCwire, acceso: agosto 12, 2025, https://www.hpcwire.com/2024/11/14/nist-issues-draft-post-quantum-cryptography-transition-strategy-and-timeline/
124. atis.org, acceso: agosto 12, 2025, https://atis.org/resources/quantum-technologies-and-the-cryptographic-threat-timeline-a-strategic-

overview/#:~:text=While%20current%20expert%20estimates%20suggest,timeline%20may%20be%20overly%20conservative.
125. The timelines: when can we expect useful quantum computers?, acceso: agosto 12, 2025, https://introtoquantum.org/essentials/timelines/
126. Quantum Technologies and the Cryptographic Threat Timeline: A Strategic Overview - ATIS, acceso: agosto 12, 2025, https://atis.org/resources/quantum-technologies-and-the-cryptographic-threat-timeline-a-strategic-overview/