# TRABAJO DE INVESTIGACIÓN FUNDAMENTOS DE LOS COMPUTADORES

CRIPTOGRAFIA POST-CUANTICA (PQC)


***GENAR AGUIRRE MURUA***

# ÍNDICE

# 1.Introducción y Objetivos

## 1.1 Introducción

En este trabajo de investigación afrontaré un tema relacionado con los computadores y la ciberseguridad. Dicho tema para abordar es el de la criptografía Post-Cuántica. El cual es un campo de estudio que consiste en desarrollar algoritmos y técnicas criptográficas que resistirán los ataques de los computadores cuánticos.

En la actualidad, la computación cuántica parece ser algo novedoso y un campo de investigación que requiere madurar, pero con los años los estudios avanzan y, con esto, el conocimiento en este campo. También es un tema que apunta a ser el futuro de la seguridad en las comunicaciones, pero no por ello hay de desechar todo el trabajo hecho con la tecnología actual.

Y cómo se ha mencionado antes, aunque parezca un tema actual las primeras apariciones de esta criptografía preceden a los años 80, pero es ahora cuando se le da más relevancia a su estudio desarrollando nuevos algoritmos para protegernos de las altas capacidades de los computadores cuánticos.

Hay que tener en cuenta que la computación cuántica emplea técnicas de mecánica cuántica las cuales pueden llegar a revolucionar la tecnología tal y como la conocemos.

En este trabajo sobre todo me centrare en los tipos de encriptación y los algoritmos Post cuánticos. Aunque también abordare posibles amenazas y apartados importantes.

## 1.2 Objetivos

El principal objetivo de la criptografía post cuántica es diseñar algoritmos y métodos resistentes a los computadores cuánticos y a los clásicos.

Pero para ello hay hacer diferentes planteamientos a a hora de hacer los algoritmos de cómo se hacían con la tecnología tradicional.

# 2. Algoritmos de Criptografía Post Cuántica

La informática cuántica es un tema completamente diferente a la informática tradicional, ya que realiza los cálculos empleando la mecánica cuántica como se ha mencionado en la introducción. Además, como explicare más adelante, los bits de los computadores cuánticos son diferentes a los bits tradicionales. Esto quiere decir que los computadores cuánticos son una herramienta poderosa para resolver problemas complejos.

Por lo cual los algoritmos los cuales son los fundamentos de la seguridad digital actual deben de ir acorde con la tecnología, es decir los algoritmos tradicionales no son completamente validos ante la tecnología cuántica, por ello se han creado nuevos algoritmos con capacidad de resistir los posibles ataques que salgan de la computación cuántica en un futuro.

## 2.1. Algoritmos Cuánticos

Para explicar los algoritmos post cuánticos antes habría que abordar los algoritmos cuánticos los cuales son conjuntos de instrucciones diseñados para ser ejecutados en los computadores cuánticos.

Los siguientes algoritmos son algunos de los más conocidos en la computación cuántica:

### 2.1.1 Algoritmo de Shor

Este es un tipo de algoritmo centrado en la criptografía cuántica, "*En computación cuántica, el **algoritmo de Shor** es un algoritmo cuántico para descomponer en factores un número N en tiempo O ((log N)$^3$) y espacio O(logN), así nombrado por Peter Shor." [*2]. Es decir, a diferencia de los ordenadores clásicos para los cuales la factorización de números es muy difícil de resolver, mediante este algoritmo y los ordenadores cuánticos prometen resolverlo de forma más eficiente.

#### *2.1.1.a Componentes importantes*

-La transformada cuántica de Fourier es una variante cuántica de la transformada de Fourier, lo que permite al algoritmo determinar el periodo de una función. La transformada de Fourier es importante para muchos algoritmos cuánticos ya que dependen de este, el cual se utiliza frecuentemente para acelerar los algoritmos tradicionales.

- El algoritmo emplea búsqueda de períodos y aritmética modular para determinar eficazmente el período de una función determinada con mucha certeza. La aritmética modular, un principio fundamental de la teoría de números, se emplea ampliamente en diversos campos de las matemáticas y la informática. El algoritmo de Shor lo aplica específicamente en forma de determinación del período de una función particular.

- El algoritmo de Shor en términos de velocidad y complejidad supera a cualquier algoritmo tradicional. Este algoritmo exhibe complejidad polinomial, lo que le permite resolver eficientemente la compleja tarea de factorización de enteros para números grandes. La notable velocidad del algoritmo de Shor se debe a su empleo del paralelismo cuántico, que permite la ejecución simultánea de múltiples cálculos.

#### 2.1.1.b Funcionamiento del algoritmo

El proceso comienza tomando un número compuesto y transformándolo en un estado cuántico que represente sus factores. Mediante una secuencia de operaciones cuánticas, el algoritmo determina el período de una función particular. Esta información crucial permite la factorización del número compuesto.

### 2.1.2 Algoritmo de Grover

Es un tipo de algoritmo criptográfico cuántico que se basa en la búsqueda de elementos en una base de datos no ordenada en un tiempo cuadrático. "*el **algoritmo de Grover** es un algoritmo cuántico para la búsqueda en una secuencia no ordenada de datos con N componentes en un tiempo O (N$^{1/2}$), y con una necesidad adicional de espacio de almacenamiento de O(logN) (véase notación O, Fue inventado por Lov K. Grover en 1996.)*"[4]. Es decir que un computador cuántico tardaría menos tiempo en hacer las búsquedas que un computador clásico.

#### *2.1.2.a Componentes importantes*

-Superposición: El algoritmo de Grover utiliza el concepto de superposición, un principio importantísimo de la mecánica cuántica. En la superposición, un sistema cuántico puede existir en múltiples estados simultáneamente. Lo que permite al algoritmo examinar simultáneamente todos los valores posibles de un elemento de búsqueda.

-Oráculo: Un oráculo es un circuito cuántico que actúa con la superposición y marca el elemento deseado. El oráculo modifica las amplitudes de la superposición, haciendo que la amplitud del elemento marcado aumente mientras que las otras amplitudes disminuyen.

-Amplificación de la amplitud: Después de la operación del oráculo, el algoritmo realiza una operación llamada amplificación de amplitud. Esta operación amplifica la amplitud

del elemento marcado, aumentando su probabilidad de ser medido durante el paso final del algoritmo.

-Iteración: El algoritmo de Grover itera varias veces las operaciones de oráculo y amplificación de amplitud.

*2.1.2.b Funcionamiento del algoritmo*

El algoritmo de Grover funciona utilizando los componentes anteriores, comienza aplicando el operador de difusión en el estado inicial que sería el de superposición y luego aplicaría el oráculo en el resultado.

Esto se repite el número de veces de estados posibles del conjunto de búsqueda y de esta manera se amplificaría el resultado hasta el valor más cercano a 1.

### 2.1.3 Algoritmo de Deutsch-Jozsa

Este algoritmo cuántico es uno de los primeros algoritmos diseñados para ejecutarse sobre un computador cuántico propuesto por David Deutsch y Richard Josza en 1992, el cual tiene un mejor potencial ante los algoritmos clásicos el cual aprovecha la superposición de los computadores cuánticos.

*2.1.1.a Componentes importantes*

-Superposición: Al igual que he explicado en el anterior punto del algoritmo de Grover se emplea la superposición lo que supone una ventaja fundamental para resolver problemas que impliquen múltiples posibilidades.

-Puerta de Hadamard: Esta es una puerta cuántica importante que transforma un qubit desde su base estándar a una superposición de ambos estados. Esta operación es esencial para preparar el registro cuántico en una superposición de todos los valores de entrada posibles, lo que permite al algoritmo explorar todas las combinaciones de entrada de forma eficiente.

-Función oráculo: La función oráculo representa la función booleana a evaluar. Se implementa utilizando puertas lógicas cuánticas que realizan las operaciones lógicas de la función. Al aplicar la función oráculo a la superposición de valores de entrada, el algoritmo prueba la función en todas las entradas posibles simultáneamente.

*2.1.1.b Funcionamiento del algoritmo*

El algoritmo comienza inicializando el registro cuántico en una superposición de todos los valores de entrada posibles.

Luego habría que emplear la función oráculo, que representa la función booleana que debe evaluarse, se aplica en la superposición de valores de entrada.

Una vez aplicada la función oráculo, se realiza una medición en el registro cuántico. Esto colapsa la superposición, dando como resultado un único estado qubit que representa la salida de la función para un único valor de entrada. La medición suele repetirse varias veces para obtener un resultado estadísticamente significativo.

## 2.2. Algoritmos PostCuánticos

A continuación, se expondrán 4 tipos de encriptaciones y en ellos algunos algoritmos postcuanticos.

### 2.2.1 Criptografía basada en funciones hash

Estos tipos de algoritmos son los que emplean las funciones has para generar criptografía de clave pública.

Estos se basan en la dificultad de resolver problemas matemáticos que resista ante los ataques cuánticos.

#### *2.2.1.a Algoritmo de NewHope*

Es un algoritmo que pretende diseñar un nuevo sistema de intercambio de claves, para que el cifrado en un futuro no sea vulnerable ante las computadoras cuánticas.

#### 2.2.1.a.a Componentes importantes

-Ring-Learning-with-Errors (Ring-LWE): Este es un problema matemático que sirve como base criptográfica del algoritmo NewHope. El cual consiste en resolver ecuaciones lineales sobre una estructura de anillo, en este los coeficientes están corruptos por errores aleatorios. Se cree que este problema consta de una dificultad insuperable para los ordenadores cuánticos.

-Generación de claves: En las dos partes de la transmisión de información se generan claves privadas independientemente. Estas claves se mantienen privadas durante la transferencia de datos.

-Intercambio de claves: En este caso se intercambian las claves públicas, que derivan de las claves privadas. Las claves públicas contienen información necesaria para la reconciliación de claves.

-Coeficientes de corrección de errores: Durante la transferencia también se intercambian coeficientes de corrección de errores, los cuales son valores generados aleatoriamente que se utilizan para mejorar la precisión de la reconciliación de claves.

-Reconciliación: Durante la transferencia se emplean algoritmos de reducción reticular para extraer una clave secreta compartida a partir de la información intercambiada.

-Validación de la clave secreta compartida: Para verificar la validez de la clave secreta compartida, las dos partes realizan una comprobación final para asegurarse de que comparte la misma estructura que la clave secreta original.

-Eficiencia computacional: NewHope utiliza algoritmos eficientes de reducción de retículos que minimizan la complejidad computacional del intercambio de claves, lo que permite una implementación práctica.

-Eficiencia de la comunicación: La sobrecarga de comunicación que genera el algoritmo realmente es baja, ya que exige un intercambio mínimo de datos entre las partes de la comunicación.

-Adaptabilidad a los niveles de seguridad: Este algoritmo puede adaptarse a diferentes niveles de seguridad ajustando los parámetros del problema Ring-LWE. Esto permite elegir el nivel de seguridad adecuado dependiendo de los requisitos criptográficos.

### 2.2.1.a.b Funcionamiento del algoritmo

Siguiendo los componentes clave se generan las claves privadas con el problema Ring-LWE.

Luego se intercambian las claves públicas de las dos partes, las cuales contienen la información necesaria para la reconciliación de claves. Estas son conocidas públicamente y se pueden compartir sin comprometer la clave secreta.

Las dos partes usan algoritmos de reducción para sacar la clave secreta de las claves públicas intercambiadas y de los coeficientes de corrección de errores. Entonces se usa la clave secreta para cifrar y descifrar el mensaje

Para garantizar la validez de la clave secreta compartida, las dos partes hacen una comprobación final para confirmar que comparte la misma estructura algebraica que la clave secreta original.

### *2.2.1.b Algoritmo de Kyber*

Kyber es un método de encapsulamiento de claves (KEM), el cual es un tipo primitivo de criptografía el cual establece una clave compartida a dos partes mediante un canal inseguro. Este está diseñado para ser resistente ante ataques criptoanalíticos por parte de computadoras cuánticas.

### 2.2.1.b.a Componentes importantes

-Estructura reticular: El algoritmo trabaja sobre una retícula de módulos, el cual es un conjunto finito de vectores sobre un campo finito. Esta estructura constituye la base criptográfica de operaciones.

-Problema de aprendizaje con errores (LWE): La seguridad de Kyber se basa en la intratabilidad computacional del problema LWE.

-Función pseudoaleatoria (PRF) y función de salida ampliable (XOF): Kyber utiliza una función pseudoaleatoria para generar una clave aleatoria a partir de una semilla. Se emplea una función de salida ampliable para producir una secuencia amplia de bits aleatorios a partir de una semilla.

-Funciones hash: Se utilizan dos funciones hash, para transformar escalares en polinomios. Una de ellas transforma un escalar en un polinomio de 32 bytes, mientras que el otro transforma un polinomio de 32 bytes en un par de polinomios de 32 bytes.

-Función de derivación de claves (KDF): Kyber utiliza una función de derivación de claves con la que en base a la clave secreta deriva la clave simétrica. La cual puede utilizarse para diversos fines criptográficos, como el cifrado de datos o la autenticación de mensajes.

-Transformación teórica de números (NTT) y multiplicación: Estas operaciones se utilizan para procesar los elementos de la red y realizar operaciones clave.

-Codificación y descodificación: Kyber utiliza mecanismos de codificación y descodificación para convertir entre representaciones polinómicas y matrices de bytes.

*2.2.1.b.b Funcionamiento del algoritmo*

Kyber se basa en la dureza del problema de aprendizaje con errores (LWE) sobre redes de módulos. Este problema es difícil de resolver para los ordenadores clásicos, pero se cree que puede ser resuelto por los ordenadores cuánticos.

Primero El emisor genera una clave pública y una clave secreta.

Luego el destinatario genera un nonce aleatorio y lo envía al remitente. A continuación, el remitente genera un texto cifrado, el cual se envía al destinatario.

El destinatario recibe el texto cifrado y su nonce. Utiliza su clave secreta para descifrar el texto cifrado, lo que genera una clave secreta compartida.

2.2.2 Criptografía basada en retículos

La criptografía basada en retículos es un enfoque muy prometedor de la criptografía postcuántica que utiliza las propiedades matemáticas de los retículos para construir criptográficas seguras.

*2.2.2.a Algoritmo de Crystals-Dilithium*

Es un esquema de firma digital postcuántico que utiliza la dificultad de encontrar vectores cortos en retículas. Al ser parte de Crystals utiliza un sistema parecido a Kyber

2.2.2.a.a Componentes importantes

Tiene componentes similares a los de Kyber

-Generación de claves: El firmante genera una clave pública y una clave secreta. La clave pública se utiliza para verificar las firmas, la clave secreta al contrario se utiliza para firmar mensajes.

-Firma de mensajes: El firmante firma un mensaje utilizando su clave secreta. Este proceso implica la creación de un reto aleatorio, el cálculo de una serie de polinomios y la selección de un vector aleatorio de una red. La firma es una combinación del reto, los polinomios y el vector seleccionado.

-Verificación del mensaje: El verificador recibe un mensaje firmado y la clave pública del firmante. Puede verificar la firma comprobando si cumple las condiciones matemáticas.

2.2.2.a.b Funcionamiento del algoritmo

Funciona igual que kyber.

El firmante genera una clave pública y una clave secreta. La clave pública puede utilizarse para verificar firmas, mientras que la clave secreta se utiliza para firmar mensajes.

El firmante firma un mensaje utilizando su clave secreta.

El verificador recibe un mensaje firmado y la clave pública del firmante. Cumpliendo las condiciones matemáticas puede verificarse.

*2.2.2.b Algoritmo de NISTPQC-Crystals*

NISTPQC-Crystals está diseñado para su uso en una variedad de aplicaciones que requieren un intercambio de claves seguro. Es conocido por el tamaño relativamente pequeño de sus claves, lo que hace que sea eficaz de desplegar y utilizar en la práctica.

2.2.2.b.a Componentes importantes

-Resistente a la cuántica: Está diseñado para ser seguro tanto en ordenadores tradicionales como cuánticos, logrando que sea una buena elección para criptografía a largo plazo.

-Claves compactas: Utiliza tamaños de clave relativamente pequeños, lo que hace que sea eficiente de implementar y utilizar.

-Funcionamiento rápido: Este es un algoritmo relativamente rápido, lo que significa

que puede ser utilizado en aplicaciones a tiempo real.

-Resistencia a la maleabilidad: Es resistente a ataques de maleabilidad, lo que significa que es difícil modificar mensajes encriptados sin ser pillado.

#### 2.2.2.b.b Funcionamiento del algoritmo

En la primera fase, dos partes acuerdan un conjunto de parámetros para el problema LWE. Estos parámetros incluyen el tamaño de la red, la distribución del ruido y la clave secreta. A continuación, las partes generan sus propias claves secretas utilizando los parámetros acordados.

En la segunda fase, las partes intercambian mediciones ruidosas de sus claves secretas. El intercambio de claves es seguro porque es difícil para un atacante espiar las mediciones y recuperar las claves secretas.

El algoritmo es un esquema de establecimiento de claves potente y versátil, muy adecuado para una gran variedad de aplicaciones. Es seguro tanto contra ordenadores clásicos como cuánticos, tiene un tamaño de clave relativamente pequeño y es rápido de utilizar.

### 2.2.3 Criptografía basada en matemáticas cuánticas

La criptografía basada en las matemáticas cuánticas es un campo que utiliza los principios de la mecánica cuántica para desarrollar algoritmos criptográficos nuevos y seguros. La criptografía cuántica ofrece varias ventajas sobre la criptografía tradicional, como su resistencia a las escuchas y su capacidad para proporcionar una seguridad inquebrantable incluso contra los ordenadores cuánticos.

#### *2.2.3.a Algoritmo de FHE*

Es un tipo de algoritmo que realiza cálculos sobre datos cifrados. Esto significa que los datos sensibles pueden compartirse y analizarse sin comprometer su confidencialidad.

A medida que los ordenadores cuánticos se vuelvan más potentes, FHE tendrá que adaptarse para ser resistente a los ataques cuánticos. Estos algoritmos se basan en diferentes problemas matemáticos y ofrecen distintos niveles de rendimiento y eficacia.

#### 2.2.3.a.a Componentes importantes

Generación de claves: Consta de una clave publica y privada. La clave privada se utiliza para descifrar, mientras que la pública para cifrar sin formato. El proceso de generación se basa en operaciones matemáticas resistentes a ataques cuánticos.

Operaciones homomórficas: Son operaciones que facilitan realizar cálculos sobre datos cifrados. Esto se hace empleando una serie de esquemas de cifrado homomórficos, los cuales admiten un tipo especifico de operación. El resultado de los cálculos también se cifra y se pueden procesar empleando el mismo esquema.

Evaluación de predicados: Es la capacidad de evaluar expresiones booleanas en datos cifrados. Lo cual se consigue usando unos esquemas de evaluación de predicados, los cuales esta diseñados para soportar un predicado especifico. El resultado también está cifrado.

Cambio de claves: Es la capacidad de cambiar entre diferentes esquemas de cifrado. Esto es necesario para el procesamiento eficaz y seguro de los datos. El cambio de claves se consigue normalmente mediante una técnica llamada bootstrapping.

#### 2.2.3.a.b Funcionamiento del algoritmo

Este algoritmo funciona en base a dos fases la de la superposición y en entrelazamiento.

La superposición permite que los qubits existan en una combinación de estados simultáneamente. Esto se puede aprovechar en los algoritmos FHE para realizar diferentes cálculos sobre datos cifrados simultáneamente.

El entrelazamiento es un fenómeno en el que los qubits quedan vinculados. Esto puede utilizarse para distribuir cálculos entre varios procesadores cuánticos, lo que permite el procesamiento en paralelo. Al entrelazar qubits, FHE puede realizar cálculos sobre datos cifrados con una velocidad y escalabilidad enormes.

### *2.2.3.b Algoritmo de LWE*

El problema del aprendizaje con errores (LWE) es un problema matemático que se considera difícil de resolver en los ordenadores tradicionales. Sin embargo, se ha demostrado que los ordenadores cuánticos pueden resolver el problema LWE de manera eficiente, lo que podría tener un impacto significativo en la criptografía.

#### 2.2.3.b.a Componentes importantes

-Entramado: Una retícula es una estructura matemática compuesta por un conjunto de vectores que cumplen algunas condiciones. En LWE, las retículas se utilizan para almacenar y procesar datos de forma segura.

-Vector de error: Un vector de error es un vector de pequeños números aleatorios que se añade a un vector secreto para crear un texto cifrado

-Reducción modular: La reducción modular es una operación matemática que divide un número por otro y recoge el resto.

-Muestreo gaussiano: Es una técnica matemática que genera números aleatorios a partir de una distribución gaussiana.

-Problema de los vectores cortos (SVP): Es un problema de retículas que está estrechamente relacionado con el problema LWE. El problema SVP consiste en encontrar el vector más corto en una retícula, que puede utilizarse para resolver el problema LWE de buena forma.

#### 2.2.3.b.b Funcionamiento del algoritmo

El algoritmo LWE utiliza una estructura reticular para almacenar y procesar datos. En LWE, las retículas se utilizan para crear un texto cifrado difícil de descifrar sin la clave secreta correcta.

Para cifrar un mensaje, el emisor genera un vector de error aleatorio y luego hace el cálculo del texto cifrado añadiendo el vector de error al mensaje y realizando una reducción modular. Lo que garantiza que el vector secreto y el vector de error se limitan a un determinado rango de valores.

El receptor pude descifrar el texto cifrado calculando el vector de error y quitándolo del texto cifrado. El vector de error se calcula restando la matriz de clave pública del texto cifrado y después una reducción modular. Para terminar, el vector de error se resta del texto cifrado para obtener el mensaje original.

### 2.2.4 Criptografía basada en Teoría de la Información

Es una rama de la criptografía que utiliza temas de la teoría de la información para crear y analizar esquemas criptográficos. La teoría de la información proporciona un marco riguroso para cuantificar y comprender la información, lo que la hace perfecta para abordar los objetivos fundamentales de la

criptografía: confidencialidad, integridad y autenticidad.

*2.2.4.a Algoritmo de McEliece*

El criptosistema McEliece es un algoritmo de cifrado asimétrico desarrollado en 1978 por Robert McEliece.

Es uno de los criptosistemas de clave pública más antiguos y estudiados, y sigue siendo una opción popular para aplicaciones que requieren una gran seguridad y eficiencia.

El criptosistema McEliece se considera resistente a los ataques cuánticos porque se basa en la descodificación de códigos Goppa con errores aleatorios, que es un problema computacionalmente difícil para los ordenadores cuánticos.

Esto se debe a que los ordenadores cuánticos pueden utilizarse para simular eficazmente ordenadores clásicos, pero no pueden resolver eficazmente problemas basados en problemas matemáticos intratables.

2.2.4.a.a Componentes importantes

-Códigos Goppa: Basados en los principios de la geometría algebraica, los códigos Goppa sirven como una forma de código de corrección de errores lineales. Estos códigos son especialmente adecuados para el cifrado McEliece debido a su capacidad para rectificar una cantidad significativa de errores utilizando una cantidad mínima de palabras clave.

El proceso de generación de claves juega un papel crucial en la determinación de los parámetros del código, que a su vez dictan la longitud de las palabras clave y la capacidad del código para corregir errores.

-Errores aleatorios: Se añaden errores aleatorios al mensaje antes de codificarlo con la clave pública. El número y la ubicación de los errores se eligen aleatoriamente, y están diseñados para dificultar que un atacante descifre el mensaje sin la clave privada.

La tasa de error es un parámetro importante del criptosistema McEliece, ya que determina la solidez de la seguridad. Una mayor tasa de error hace que el sistema sea más seguro, pero también hace que el proceso de cifrado y descifrado sea más costoso desde el punto de vista computacional.

-Codificación inversa: El proceso de codificación inversa se utiliza para descodificar el mensaje a partir del código Goppa. Esto implica corregir los errores que se introdujeron durante el proceso de codificación y recuperar el mensaje original.

El proceso de codificación inversa se basa en las propiedades algebraicas de los códigos Goppa. Es un proceso computacionalmente intensivo, pero necesario para garantizar la seguridad del criptosistema McEliece.

2.3.4.a.b Funcionamiento del algoritmo

El emisor empieza eligiendo un código Goppa de la longitud y capacidad de la corrección de errores deseados. Los parámetros del código Goppa se eligen aleatoriamente.

El emisor crea un mensaje aleatorio de longitud “k” bits. Después, el mensaje se codifica empleando una función de codificación del código Goppa. De esta manera logrando la codificación Goppa de n bits.

El emisor introduce aleatoriamente un pequeño número de errores en la codificación Goppa. Estos errores están diseñados para complicar que un atacante descifre el mensaje sin tener la clave privada.

La clave pública consiste en los parámetros del código Goppa y el mensaje codificado con errores. Esta clave pública se utiliza para cifrar los mensajes.

### *2.2.4.b Algoritmo de Niederreiter*

El algoritmo de Niederreiter es un algoritmo criptográfico post-cuántico que se basa en la teoría de la codificación para lograr la seguridad. Es una variante del criptosistema McEliece, otro algoritmo basado en códigos. Ambos algoritmos se consideran resistentes a los ataques de los ordenadores cuánticos, lo que los convierte en candidatos prometedores para futuros protocolos de comunicación seguros.

#### 2.2.4.b.a Componentes importantes

-Código Goppa: Es la base criptográfica del algoritmo Niederreiter. Su capacidad de corrección de errores permite al algoritmo soportar interrupciones en los mensajes transmitidos.

-Matriz generadora: Es un componente crucial de la clave pública, mediante la matriz generadora facilita el cifrado y descifrado de los mensajes. Además, transforma los mensajes en la estructura de código Goppa, insertando errores controlados los que se pueden solucionar al descifrarlo.

-Matriz de comprobación de paridad: Ayuda a detectar y corregir errores durante el proceso de descifrado. Al examinar el mensaje codificado, esta matriz identifica y rectifica los errores introducidos durante la transmisión.

-Problema del subgrupo oculto (HSP): La seguridad del algoritmo de Niederreiter se basa en la dificultad del problema, el cual es un problema computacional que sigue siendo enorme para los computadores cuánticos. Descifrar mensajes con el algoritmo implica resolver el problema, lo que lo hace resistente a los ataques cuánticos.

#### 2.2.4.b.b Funcionamiento del algoritmo

El algoritmo de Niederreiter utiliza códigos Goppa, los cuales tienen ciertas propiedades que los hacen muy adecuados para aplicaciones criptográficas.

Para cifrar primero hay que generar una clave publica mediante el Código Goppa y una matriz generadora.

Después se pasa a la codificación donde el emisor encripta un mensaje codificándolo en código Goppa e utilizando la matriz generadora, este proceso introduce errores en el mensaje los cuales quedan enmascarados por las capacidades de corrección de errores.

Luego el texto cifrado, que es el mensaje codificado, se transmite al destinatario.

En cambio, para el proceso de descifrar se empieza generando una clave privada, la cual en una matriz de comprobación de paridad para el código Goppa.

Después el destinatario recibe el texto cifrado e intenta descodificarlo utilizando la clave privada. La capacidad de corrección de errores del código permite al destinatario lograr el código original independientemente si se a corrompido durante la transmisión o no.

# 3. Amenazas Cuánticas de la Criptografía Actual y soluciones

## 3.1 Amenaza Principal

La computación cuántica es un tema muy novedoso, es decir, no se tiene tanto conocimiento como podríamos tener a la computación tradicional. Por ello puede ser una amenaza para los algoritmos y sistemas actuales los cuales no están preparados para la computación cuántica, ya que la computación cuántica emplea qbits en vez de bits. Los bits son binarios y son 1's y 0's, en cambio los qbits pueden ser 1's, 0's y una superposición que también puede ser 0's y 1's.

Teniendo en cuenta que la algunos de los algoritmos actuales se basan en la dificultad de resolver factores con números grandes como pude llegar a ser "RSA" por ejemplo, con la tecnología cuántica esa dificultad se resume por lo que todo cambia y es la mayor amenaza respecto a la criptografía actual.

Para ello se han planteado varias posibles soluciones:

## 3.2 Soluciones

-Criptografía computación postcuántica: Seria como inventar una cerradura la cual ni los computadores cuánticos sean capaces de forzarlo. Es decir, resolver problemas matemáticos difíciles que sean muy difíciles de resolver incluso para los computadores cuánticos.

-Distribución de claves cuánticas: La computación cuántica y la ciberseguridad generaron una clave que se autodestruye. Es decir, en el momento de envíos de mensajes secretos que el mensaje se borre en caso de que algún indeseable intente acceder a él. Esto consta en emplear reglas de física cuántica para mantener la seguridad en las claves criptográficas.

-Sistemas criptográficos híbridos: Esto seria como tener una cerradura tradicional y además una nueva cerradura para la cuántica. Incluso si en el caso de que alguien elige una de las dos entradas y la rompe no podrá acceder sin la otra.

-Actualizaciones y bifurcaciones continuas de la red: Se hacen actualizaciones o cambios en la red para ocultarse de los atacantes.

-Tamaños de clave aumentados: Hacer que las claves del mundo criptográfico sean más grandes y difíciles es un método para darle mayor seguridad. Con esto se gana tiempo hasta que los computadores cuánticos avancen y mejoren.

# 4. Estándares y Protocolos

## 4.1Estandares

Actualmente se ha reconocido la necesidad y urgencia de la criptografía Postcuantica, por ello muchas organizaciones en el mundo han lanzado iniciativas de estandarización para evaluar y elegir algoritmos PostCuanticos como se han explicado anteriormente para su adopción generalizada. La más destacada de las iniciativas ha sido el proyecto de estandarización liderado por el NIST en Estados Unidos.

Este proyecto lleva en activo desde el año 2016 y ha invitado a diferentes desarrolladores e investigadores para que presenten sus algoritmos para evaluarlos. Este proyecto se ha sometido a varias rondas de evaluación, centrándose en los requisitos de estandarización, seguridad y eficacia de cada algoritmo.

## 4.2 Proyecto del 2022

El pasado año 2022 se hizo un proyecto de normalización por parte del NIST en el cual en la ronda final se anunciaron 17 algoritmos participantes.

Estos algoritmos representan diferentes enfoques de la criptografía postcuantica, en los que se usan problemas matemáticos como retículos.

## 4.3 Protocolos

Aunque la estandarización de la criptografía postcuantica haya priorizado los algoritmos individuales, también es necesario tener en cuenta los protocolos. Los cuales integran varios algoritmos y definen las interacciones entre las partes implicadas en la comunicación.

Estos protocolos deben tener en cuenta aspectos prácticos como la gestión de claves, la eficacia de las operaciones criptográficas y la compatibilidad con las infraestructuras de comunicación existentes. Los esfuerzos en la estandarización también están abordando dichos aspectos para asegurar la adopción fluida y segura.

# 5. Retos de Implementación

-Idoneidad de los algoritmos: La selección de algoritmos válidos para aplicaciones específicas es importantísimo, teniendo en cuenta diferentes factores como el rendimiento, la seguridad y la compatibilidad.

-Evaluación de algoritmos: La evaluación completa de los algoritmos es importantísimos para valorar su resistencia a ataques conocidos, vulnerabilidades potenciales y garantizar la seguridad a largo plazo.

-Retos de integración: La integración de algoritmos en bibliotecas criptográficas, protocolos y aplicaciones existentes puede resultar difícil y requerir de cambios en los componentes de software y hardware.

-Sobrecarga de rendimiento: Los algoritmos cuánticos suelen presentar una sobrecarga de rendimiento en comparación con los tradicionales, por lo que se requieren técnicas de optimización para mantener los niveles de rendimiento estables.

-Ausencia de norma universal: La falta de una norma única y universalmente adoptada para los algoritmos postcuanticos puede dificultar la integración y dificultar su adopción en diferentes sistemas y aplicaciones.

-Proceso de estandarización: El proceso de estandarización de los algoritmos postcuanticos debe ser riguroso para garantizar la selección de soluciones sólidas.

-Sistemas heredados: La actualización de los sistemas y aplicaciones heredados para

incorporar la criptografía postcuantica puede resultar difícil debido a problemas de compatibilidad y a la necesidad de realizar pruebas y validaciones completas.

-Migración de infraestructuras de clave pública (PKI): El paso de las PKI existentes para que admitan certificados y mecanismos de autenticación basados en criptografía postcuantica requiere una planificación y coordinación cuidadosas.

-Requisitos de hardware: Los algoritmos post cuánticos pueden llegar a requerir más recursos informáticos, como mayor potencia de CPU y memoria.

-Conocimientos necesarios: El desarrollo e implementación de soluciones de la criptografía postcuantica requieren conocimientos más especializados.

# 6. Conclusión

El mundo de la computación cuántica es algo fascinante, aunque sea algo complicado de comprender ya que esta directamente relacionado con la mecánica cuántica lo que es algo muy difícil de entender.

Aunque sea un tema muy difícil la tecnología cuántica va avanzando por ello es importantísimo que la seguridad en ese ámbito también avance al mismo ritmo, y para ello hay muchas organizaciones y gente trabajando en los algoritmos criptográficos para lograr esa seguridad para cuando la computación cuántica se haga realidad en un futuro.

Hoy en día, no es una gran amenaza ya que hay muy pocos ordenadores cuánticos, y los que hay tienen relativamente poca cantidad de qbits, pero ya hay organizaciones que avanzan y se espera que en 2025 la empresa IBM presente un computador que alcance los 4000 qbits. Es decir, de cara al futuro es un peligro, por ello es necesario avanzar con la investigación de algoritmos capaces de frenar a los ordenadores cuánticos, y los anteriormente mencionados pueden ser el principio de la seguridad cuántica.

¿Pero realmente se puede conseguir un algoritmo perfecto?

No, al igual que con los ordenadores clásicos no hay seguridad perfecta. Por ello es necesario investigar para lograr la mayor protección posible ante los futuros ataques cuánticos.

En conclusión, estos algoritmos son el futuro de la ciberseguridad y con esta investigación he visto su verdadera importancia y la necesidad de conocer más sobre estas tecnologías.

# 7. Vocabulario

-Algoritmo: Un algoritmo es un conjunto de instrucciones definidas que facilita solucionar problemas mediante operaciones sistemáticas y finitas.

*Link:* https://es.wikipedia.org/wiki/Algoritmo

-Mecánica cuántica: Es una de las ramas principales de la física cuántica que estudia la naturaleza de los átomos.

*Link:* https://es.wikipedia.org/wiki/Mec%C3%A1nica_cu%C3%A1ntica

-Transformación de Fourier: Es una transformación matemática utilizada para transformar señales entre el dominio del tiempo y el de la frecuencia.

*Link:* https://es.wikipedia.org/wiki/Transformada_de_Fourier

-Aritmética modular: Es un sistema aritmético para clases de equivalencia de números enteros llamados clases de congruencia

*Link:* https://es.wikipedia.org/wiki/Aritm%C3%A9tica_modular

-Determinación del periodo: Es el proceso de identificación del intervalo de tiempo en el que ocurre un suceso.

-Paralelismo cuántico: Esta es una característica clave de la computación cuántica que permite acelerar exponencialmente ciertos tipos de cálculos.

*Link:* https://www.tomorrow.bio/es/post/la-computaci%C3%B3n-cu%C3%A1ntica-explicada-2023-06-4669699767-quantum

-Tiempo cuadrático: Es un tipo de complejidad algorítmica que se refiere a un algoritmo del cual su tiempo de ejecución aumenta de manera proporcional al cuadrado del tamaño de la entrada.

Link: https://es.wikipedia.org/wiki/Complejidad_temporal

-Superposición: Es un principio fundamental de la mecánica cuántica en el que un sistema físico, existe en parte en todos sus teóricamente posibles estados de forma simultánea

*Link:* https://es.wikipedia.org/wiki/Superposici%C3%B3n_cu%C3%A1ntica

-Retículos: Es una estructura matemática que se utiliza para modelar proposiciones cuánticas. Se puede definir como un conjunto de subespacios cerrados de un espacio de Hilbert, con la relación de orden dada por la inclusión.

*Link:* https://es.wikipedia.org/wiki/Ret%C3%ADculo_(matem%C3%A1ticas)

-Homomorfico: Un tipo de cifrado el cual es capaz de realizar una operación algebraica concreta sobre un texto original.

*Link:* https://es.wikipedia.org/wiki/Cifrado_homom%C3%B3rfico

-Nonce: Es un numero arbitrario el cual es posible emplear una sola vez en una comunicación criptográfica.

*Link:* https://es.wikipedia.org/wiki/Nonce

-Bootstrapping: Es una técnica de remuestreo el cual se utiliza para aproximar la distribución en el muestreo de un estadístico.

*Link:*
https://es.wikipedia.org/wiki/Bootstrapping_(estad%C3%ADstica)

-Reducción modular: Esta es una operación matemática la cual se emplea para simplificar un numero en relación con un módulo dado.

*Link:*
https://en.wikipedia.org/wiki/Modular_arithmetic

-Códigos Goppa: Son una familia de códigos correctores de errores lineales, se basan en la teoría de curvas algebraicas.

*Link:*
https://en.wikipedia.org/wiki/Algebraic_geometry_code

# 8. Bibliografía

[1] https://es.wikipedia.org/wiki/Criptografía_postcuántica

[2] https://es.wikipedia.org/wiki/Algoritmo_de_Shor

[3]https://www.tomorrow.bio/es/post/qu%C3%A9-es-el-algoritmo-de-shor-s-2023-06-4669709562-quantum

[4] https://es.wikipedia.org/wiki/Algoritmo_de_Grover

[5] https://es.wikipedia.org/wiki/Algoritmo_de_Deutsch-Jozsa

[6] https://www.dotforce.es/criptografia-post-cuantica/

[7] https://openaccess.uoc.edu/bitstream/10609/89026/6/alvaroreyesTFM1218memoria.pdf

[8] https://es.wikipedia.org/wiki/Criptograf%C3%ADa_cu%C3%A1ntica#:~:text=La%20criptograf%C3%ADa%20cu%C3%A1ntica%20es%20la,se%20public%C3%B3%20el%20primer%20protocolo.

[9] https://theblackboxlab.com/2022/04/18/criptografia-cuantica-que-es-y-uso/

[10] https://www.bbvaopenmind.com/tecnologia/mundo-digital/entender-la-criptografia-cuantica/

[11] https://www.computing.es/infraestructuras/en-que-consiste-la-encriptacion-cuantica/

[12] https://grupooesia.com/insight/criptografia-cuantica-y-su-impacto-en-nuestra-ciberseguridad/

[13] https://es.wikipedia.org/wiki/Criptograf%C3%ADa_postcu%C3%A1ntica

[14] https://computerhoy.com/reportajes/tecnologia/presente-futuro-computacion-cuantica-1152893

[15] La amenaza cuántica: La computación cuántica y la criptografía | CIBERCRIMEN | CSO España (computerworld.es)

[16] Amenazas de la computación cuántica para la criptografía y sus soluciones • Blog Cryptomus

[17] El futuro de la ciberseguridad: Criptografía Post-Cuántica (PQC) (fundacionbankinter.org)

[18] Guía completa de criptografía y cifrado resistentes a los ataques cuánticos (entrust.com)

[19] https://www.linkedin.com/pulse/algoritmo-de-grover-y-el-papel-fundamental-del-or%C3%A1culo-laguna/?originalSubdomain=es

[20] https://computacioncuantica.blogspot.com/2010/02/amplificacion-de-amplitud.html

[21] https://www.nist.gov/programs-projects/post-quantum-cryptography

[22] https://www.nist.gov/blogs/taking-measure/post-quantum-cryptography-qa-nists-matt-scholl

[23] https://en.wikipedia.org/wiki/Ring_learning_with_errors

[24]

https://research.nccgroup.com/2022/07/13/nist-selects-post-quantum-algorithms-for-standardization/

[25]
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

[26]
https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/

[27] https://eprint.iacr.org/2015/1092.pdf

[28]
http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf

[29]
https://www.sciencedirect.com/book/9780128096437/information-security-science

[30] https://csrc.nist.gov/projects/post-quantum-cryptography

[40]
(https://en.wikipedia.org/wiki/Niederreiter_cryptosystem