



UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y  
DISEÑO INDUSTRIAL

Grado en Ingeniería Electrónica Industrial y Automática

**TRABAJO FIN DE GRADO**

**ESTUDIO COMPARATIVO DE  
DIFERENTES ALGORITMOS DE  
ENCRIPCIÓN PARA  
COMUNICACIONES INDUSTRIALES**

Bogurad Barański Barańska

*Cotutor:* Basil Mohammed Al-Hadithi

*Departamento:* ingeniería eléctrica,

electrónica, automática y física aplicada.

*Tutor:* Roberto Gonzalez Herranz

*Departamento:* ingeniería eléctrica,

electrónica, automática y física aplicada.

Madrid, Septiembre, 2025





UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y  
DISEÑO INDUSTRIAL

Grado en Ingeniería Electrónica Industrial y Automática

**TRABAJO FIN DE GRADO**

**TÍTULO DEL TRABAJO**

Firma Autor

*Firma Tutor*



Copyright ©2025. Bogurad Barański Barańska

Esta obra está licenciada bajo la licencia Creative Commons

Atribución-NoComercial-SinDerivadas 3.0 Unported (CC BY-NC-ND 3.0). Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-nd/3.0/deed.es> o envíe una carta a Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, EE.UU.

Todas las opiniones aquí expresadas son del autor, y no reflejan necesariamente las opiniones de la Universidad Politécnica de Madrid.



**Título:** Estudio comparativo de diferentes algoritmos de encriptación para comunicaciones industriales

**Autor:** Bogurad Barański Barańska

**Tutor:** Roberto Gonzalez Herranz

## EL TRIBUNAL

Presidente:

Vocal:

Secretario:

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el día ..... de ..... de ... en ....., en la Escuela Técnica Superior de Ingeniería y Diseño Industrial de la Universidad Politécnica de Madrid, acuerda otorgarle la CALIFICACIÓN de:

VOCAL

SECRETARIO

PRESIDENTE





# Agradecimientos

Agradezco a .....



# Resumen

Este proyecto se resume en.....

**Palabras clave:** palabraclave1, palabraclave2, palabraclave3.



# Abstract

In this project...

**Keywords:** keyword1, keyword2, keyword3.



# Índice general

<b>Agradecimientos</b>	<b>IX</b>
<b>Resumen</b>	<b>XI</b>
Palabras clave: . . . . .	XI
<b>Abstract</b>	<b>XIII</b>
Keywords: . . . . .	XIII
<b>Índice</b>	<b>XVII</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Motivación del proyecto . . . . .	1
1.2. Objetivos . . . . .	1
1.3. Herramientas utilizadas . . . . .	2
1.3.1. LaTeX [1] . . . . .	2
1.3.2. TikzMaker [2] . . . . .	2
1.3.3. C [3] y C++ [4] . . . . .	2
1.3.4. Microprocesador CY8CPROTO-063-BLE [5] . . . . .	2
1.4. Estructura del documento . . . . .	2
<b>2. Estado del arte</b>	<b>3</b>
<b>3. Fundamentos generales</b>	<b>5</b>
3.1. Introducción . . . . .	5
3.2. Algoritmos de Hashing . . . . .	5
3.3. Métodos clásicos de cifrado asimétrico . . . . .	5
3.3.1. Algoritmo Rivest-Shamir-Adleman (RSA) . . . . .	5
3.3.2. Criptografía en Curvas Elípticas (ECC) . . . . .	5
3.3.3. Algoritmo de Shore . . . . .	5
3.4. Fundamentos de seguridad de los algoritmos . . . . .	5
3.4.1. Generación de números aleatorios criptográficamente seguros . . . . .	5
3.4.2. Indistinguibilidad bajo ataque de texto cifrado adaptable IND-CCA2 . . . . .	5
3.4.3. Transformadas Fujisaki-Okamoto . . . . .	5
3.5. Funcionamiento básico de los algoritmos postcuánticos . . . . .	6
3.5.1. CRYSTALS-Kyber . . . . .	6
3.5.1.1. Transformada Teórica de Números o Number Theoretic Transform (NTT) . . . . .	7

3.5.1.2.	Aprendizaje Con Errores o Learning With Errors (LWE) . . . . .	10
	LWE en anillos . . . . .	11
	Aplicación del R-LWE para el intercambio de claves públicas . . . . .	12
	Seguridad basada en retículas ideales . . . . .	12
3.5.1.3.	Fundamentos de seguridad de Kyber . . . . .	12
	Seguridad esperada . . . . .	12
	Análisis respecto a ataques conocidos . . . . .	12
3.5.1.4.	Algoritmos principales . . . . .	12
3.5.2.	SABER . . . . .	12
3.5.3.	Hamming Quasi-Cyclic (HQC) . . . . .	12
3.5.4.	Bit Flipping Key Encapsulation (Bike) . . . . .	12
<b>4.</b>	<b>Desarrollo</b>	<b>13</b>
4.1.	Implementación comunicación serie . . . . .	13
4.1.1.	Parámetros generales y formato mensajes . . . . .	13
4.1.2.	Implementación en el ordenador . . . . .	13
4.1.3.	Implementación en el microprocesador . . . . .	13
4.2.	Estructura y API para los algoritmos de cifrado asimétrico . . . . .	13
4.2.1.	Kyber . . . . .	13
4.2.2.	Saber . . . . .	13
4.2.3.	Bike . . . . .	13
4.2.4.	HQC . . . . .	13
4.3.	Implementación algoritmos en el PC . . . . .	13
4.3.1.	Compilación en librerías . . . . .	13
4.3.2.	Diagrama de uso . . . . .	13
4.3.3.	Diagrama funcional . . . . .	13
4.3.4.	Diagrama de clases . . . . .	13
4.4.	Implementación de algoritmos en el microcontrolador . . . . .	13
4.4.1.	Diagrama de uso . . . . .	13
4.4.2.	Diagrama funcional . . . . .	13
4.5.	Implementación del intercambio de claves. Creación del secreto compartido . . . . .	13
4.5.1.	Modelo 1 . . . . .	14
4.5.2.	Modelo 2 . . . . .	14
4.5.3.	Modelo 3 . . . . .	14
4.6.	Tests de rendimiento realizados . . . . .	14
<b>5.</b>	<b>Resultados y discusión</b>	<b>15</b>
5.1.	Resultados . . . . .	15
5.1.1.	(No sé si lo metere) Resultado de ejecución de los algoritmos clásicos . . . . .	15
5.1.1.1.	RSA . . . . .	15
5.1.1.2.	ECC . . . . .	15
5.1.2.	Resultados de ejecución de los algoritmos post-cuánticos . . . . .	15
5.1.2.1.	Kyber . . . . .	15
5.1.2.2.	Saber . . . . .	15



5.1.2.3.	HQC . . . . .	15
5.1.2.4.	Bike . . . . .	15
5.1.3.	Resultados de los distintos modelos de comunicación . . . . .	15
5.1.3.1.	Modelo 1 . . . . .	15
5.1.3.2.	Modelo 2 . . . . .	15
5.1.3.3.	Modelo 3 . . . . .	15
5.2.	Discusión . . . . .	15
5.2.1.	Comparativa entre los distintos algoritmos post-cuánticos ana- lizados . . . . .	15
5.2.2.	Comparativa entre los distintos modelos de comunicación . . .	15
<b>6.</b>	<b>Conclusiones</b>	<b>17</b>
6.1.	Conclusión . . . . .	17
6.2.	Desarrollos futuros . . . . .	17
	<b>Bibliografía</b>	<b>19</b>



# Índice de figuras

3.1. Representación del cálculo de un producto de polinomios mediante NTT en comparación con los algoritmos clásicos. . . . .	10
--	----



# Índice de tablas

- 3.1. Tabla con un ejemplo numérico del calculo del valor  $b$  necesario para el problema LWE tanto en el caso puro como en la estructura de anillo de Kyber para ver como efectivamente en la clave pública  $(a, b)$  el tamaño es menor. En este ejemplo se trabaja en  $\mathbb{Z}_{17}$  y  $X^2 + 1$ . . . . 11



# Siglas

DFT	Transformada Discreta de Fourier. XIX, 8
IND-CCA2	Indistinguibilidad bajo ataque de texto cifrado adaptable. XV, XIX, 5
LWE	Aprendizaje Con Errores. XVI, XIX, 10
NTT	Transformada Teórica de Números. XV, XVII, XIX, 7–10





# Capítulo 1

## Introducción

### 1.1. Motivación del proyecto

En el ámbito de las comunicaciones industriales, la seguridad en el intercambio de información es un aspecto crítico, especialmente ante el avance de la computación cuántica y su impacto en los algoritmos criptográficos actuales. Este trabajo se enfoca en el análisis, implementación y evaluación de algoritmos de cifrado asimétrico post-cuántico en sistemas embebidos, con el objetivo de garantizar la seguridad de los protocolos de comunicación en un entorno industrial. Se realiza un estudio detallado de los fundamentos matemáticos de los algoritmos asimétricos clásicos y su vulnerabilidad frente al algoritmo de Shor, así como de los nuevos esquemas criptográficos diseñados para resistir ataques cuánticos.

El cifrado asimétrico es esencial para establecer claves seguras en protocolos de intercambio de claves, permitiendo así la utilización de cifrado simétrico en las comunicaciones industriales. Esto es particularmente relevante en sistemas de control en línea, donde el cifrado simétrico debe operar dentro del bucle de control en tiempo real, garantizando tanto seguridad como eficiencia.

Para ello, en este trabajo se comparan diferentes candidatos propuestos en el estándar NIST para evaluar su rendimiento en términos de velocidad, consumo de recursos y nivel de seguridad.

### 1.2. Objetivos

Para realizar el proyecto, se proponen los siguientes objetivos:

- Estudiar los fundamentos matemáticos de los métodos de cifrado asimétrico clásicos (no seguros cuánticamente) y modernos (seguros cuánticamente).
- Analizar el algoritmo de Shor y su impacto en la seguridad del cifrado asimétrico clásico.
- Implementar un sistema de comunicación entre un PC y un microcontrolador para el intercambio de claves seguras.
- Desarrollar e integrar los siguientes algoritmos de cifrado asimétrico post-cuántico en un microcontrolador y PC:

- Kyber
  - Saber
  - HQC
  - Bike
- Comparar el rendimiento de los algoritmos de cifrado post-cuántico evaluando velocidad, consumo de recursos y seguridad.
  - Estudiar la necesidad de implementar estos algoritmos en FPGAs en caso de que en el microcontrolador el rendimiento no fuera aceptable.
  - Implementar y diseñar un sistema de intercambio de claves que permita la escalabilidad de la solución.

### 1.3. Herramientas utilizadas

#### 1.3.1. LaTeX [1]

Se ha preferido el uso de  $\text{\LaTeX}$  debido a la facilidad que ofrece para el maquetado de textos, superando a otras herramientas de elaboración de documentos. Además,  $\text{\LaTeX}$  permite crear figuras vectorizadas, representar correctamente ecuaciones y ubicar adecuadamente figuras, tablas y bibliografía.

#### 1.3.2. TikzMaker [2]

Esta herramienta permite crear figuras vectorizadas de  $\text{\LaTeX}$  mediante el paquete de circuitikz. Su principal ventaja radica en la interfaz gráfica que proporciona y en la facilidad para elaborar figuras.

#### 1.3.3. C [3] y C++ [4]

#### 1.3.4. Microprocesador CY8CPROTO-063-BLE [5]

### 1.4. Estructura del documento

A continuación y para facilitar la lectura del documento, se detalla el contenido de cada capítulo:

- En el capítulo 1 se realiza una introducción.
- En el capítulo 2 se estudia trabajos realizados con relación al tema.
- En el capítulo 3 se desarrollan los fundamentos matemáticos del proyecto.
- En el capítulo 4 se describe la implementación de los algoritmos.
- En el capítulo 5 se presentan y analizan los resultados obtenidos en el capítulo anterior como consecuencia de ejecutar el software realizado.
- En el capítulo 6 se realiza una conclusión.

## Capítulo 2

# Estado del arte

Los artículos que de momento tengo que son relevantes mencionar, lo haré después de los fundamentos: [6] [7] [8] [9] [10] [11] [12] [?] [13] [14] [15] [16] [17]



## Capítulo 3

# Fundamentos generales

En este capítulo se desarrollan las bases matemáticas de los distintos algoritmos a implementar.

### 3.1. Introducción

### 3.2. Algoritmos de Hashing

Para elaborar esta seccion se sigue la seccion de recomendaciones del nist [18]

### 3.3. Métodos clásicos de cifrado asimétrico

#### 3.3.1. Algoritmo Rivest-Shamir-Adleman (RSA)

#### 3.3.2. Criptografía en Curvas Elípticas (ECC)

#### 3.3.3. Algoritmo de Shore

Generico: [19] ECC: [20] RSA: [21]

### 3.4. Fundamentos de seguridad de los algoritmos

Recomendaciones NIST para intercambio seguro de claves [22]

#### 3.4.1. Generación de números aleatorios criptográficamente seguros

#### 3.4.2. Indistinguibilidad bajo ataque de texto cifrado adaptable IND-CCA2

#### 3.4.3. Transformadas Fujisaki-Okamoto

[23]

### 3.5. Funcionamiento básico de los algoritmos postcuánticos

En esta sección se describe el funcionamiento de los algoritmos postcuánticos analizados en este trabajo. Dado que no se desarrollaron implementaciones propias, sino que se utilizó el código proporcionado por el NIST en la tercera [24] y cuarta [25] ronda del proceso de estandarización, resulta apropiado presentar su funcionamiento aquí en lugar de en la sección de desarrollo.

#### 3.5.1. CRYSTALS-Kyber

Se utilizará la misma notación empleada en el artículo [26]. El conjunto de los enteros sin signo de 8 bits se denota por  $\mathcal{B} = \{0, \dots, 255\}$ . Para representar vectores de tamaño  $k$ , se utiliza la notación  $\mathcal{B}^k$ , mientras que para vectores de tamaño arbitrario se emplea  $\mathcal{B}^*$ .

Para trabajar con estos vectores, se utiliza el símbolo  $\|$  para denotar la concatenación de dos cadenas, y la notación  $+k$  para indicar el desplazamiento de  $k$  bytes desde el inicio de una cadena. Por ejemplo, si se tiene una cadena  $a$  de longitud  $l$  y se concatena con una cadena  $b$ , se obtiene:

$$c = a\|b \quad (3.1)$$

Entonces:

$$b = c + l \quad (3.2)$$

Para denotar vectores, se utiliza la notación  $v[i]$ , donde  $v$  es un vector columna e  $i$  indica la posición del elemento (empezando desde 0, si no se indica lo contrario). Para las matrices, se emplea la notación  $A[i][j]$ , donde  $i$  representa la fila y  $j$  la columna. La transpuesta de una matriz  $A$  se denota como  $A^T$ .

Se denota mediante  $\lfloor x \rfloor$  el redondeo de  $x$  al entero más cercano. Por ejemplo:  $\lfloor 2,3 \rfloor = 2$ ,  $\lfloor 2,5 \rfloor = 3$  y  $\lfloor 2,8 \rfloor = 3$ .

Para las reducciones modulares se emplean dos tipos: una centrada en cero y otra correspondiente a la reducción modular estándar. Para la reducción modular centrada en cero, sea  $\alpha$  un entero par. Esta operación se define como:

$$r' = r \bmod^{\pm} \alpha \implies -\frac{\alpha}{2} < r' \leq \frac{\alpha}{2} \quad (3.3)$$

Mientras que la reducción modular estándar se denota como:

$$r' = r \bmod^{+} \alpha \implies 0 \leq r' < \alpha \quad (3.4)$$

Finalmente, se denota mediante  $s \leftarrow S$  la selección de  $s$  de manera uniformemente aleatoria del conjunto  $S$ . Si  $S$  representa una distribución de probabilidad, entonces  $s$  se selecciona de acuerdo con dicha distribución.

**3.5.1.1. Transformada Teórica de Números o Number Theoretic Transform (NTT)**

Para acelerar las operaciones de multiplicación en el esquema basado en retículas, se utiliza la Transformada Teórica de Números (NTT, por sus siglas en inglés), la cual permite reducir la complejidad temporal de la multiplicación de polinomios desde  $\mathcal{O}(n^2)$ , correspondiente al método tradicional, hasta  $\mathcal{O}(n \log(n))$ . Para más detalles, consúltese [27].

Antes de pasar a explicar el funcionamiento de este método es relevante aclarar que se trabaja sobre el siguiente anillo de polinomios para realizar las operaciones, denotado mediante  $R_q$ :

$$R_q := \frac{\mathbb{Z}_q[X]}{X^n + 1} \quad (3.5)$$

En la implementación especificada de Kyber, según el artículo [26], se utiliza un valor de  $q = 3329$  y  $n = 256$ . Esta elección es esencial para permitir el uso de la multiplicación mediante la Transformada Teórica de Números (NTT), la cual requiere que  $n|(q-1)$ , es decir, que  $n$  divida a  $(q-1)$ . Esta condición garantiza la existencia de  $n$  raíces enésimas de la unidad en  $\mathbb{Z}_q$ , lo cual es necesario para definir la NTT. La validez de esta afirmación se fundamenta en el siguiente teorema [28]:

**Teorema 1** *Para  $n, q > 1$ , el cuerpo  $\mathbb{Z}_q$  tiene una raíz enésima de la unidad si y solo si  $n|(q-1)$*

**Demostración 1** *Si  $\omega$  es una raíz enésima de la unidad en el conjunto  $\mathbb{Z}_q$ , entonces el conjunto:*

$$\Omega = \{1, \omega, \omega^2, \dots, \omega^{n-1}\} \quad (3.6)$$

*forma un subgrupo cíclico  $H$  del grupo multiplicativo  $G_{q-1}$ . Por el Teorema de Lagrange, se concluye que el orden de  $H$  divide al orden de  $G_{q-1}$ , es decir,  $n | (q-1)$ .*

*Dado que  $G_{q-1}$  es también un grupo cíclico, existe un generador  $\alpha$  tal que, por el pequeño teorema de Fermat, se cumple:*

$$\alpha^{q-1} = 1 \quad (3.7)$$

*Por lo tanto, el grupo  $G_{q-1}$  puede escribirse como:*

$$G_{q-1} = \{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\} \quad (3.8)$$

*Si se define  $\omega$  como:*

$$\omega = \alpha^{\frac{q-1}{n}}, \quad (3.9)$$

*entonces:*

$$\omega^n = \alpha^{q-1} = 1, \quad (3.10)$$

*y además, para todo  $0 < k < n$ , se cumple:*

$$k \cdot \frac{q-1}{n} < q-1 \quad \Rightarrow \quad \omega^k \neq 1. \quad (3.11)$$

*Por lo tanto,  $\omega$  es una raíz enésima de la unidad en  $\mathbb{Z}_q$ .*

Por tanto, el polinomio  $X^{256} + 1$  se puede factorizar sobre el cuerpo  $\mathbb{Z}_q$ . En la implementación concreta del esquema Kyber, este polinomio se descompone en 128 factores cuadráticos.

A este polinomio se le aplica la transformada NTT a sus coeficientes, la cual no es más que una variación de la DFT aplicada a cuerpos finitos  $\mathbb{Z}_q$  y aplicada a polinomios de grado  $n$ . Para ello, se definen dos operaciones fundamentales:

1. La transformada directa:

$$\hat{a}_j = \sum_{i=0}^{n-1} \phi^{i(2j+1)} a_i \mod q \quad (3.12)$$

2. La transformada inversa:

$$a_i = n^{-1} \sum_{j=0}^{n-1} \phi^{-i(2j+1)} \hat{a}_j \mod q \quad (3.13)$$

Donde  $\phi$  es un valor tal que  $\phi^2 = \omega$ , con  $\omega$  una raíz enésima de la unidad en  $\mathbb{Z}_q$  y  $n^{-1}$  es la inversa multiplicativa de  $n$  en  $\mathbb{Z}_q$ .

A continuación, se presenta un ejemplo extraído de [27] para ilustrar su funcionamiento. Sea el polinomio  $G(x) = 5 + 6x + 7x^2 + 8x^3$ , cuyo vector de coeficientes es  $g = [5, 6, 7, 8]$ . Trabajando en el anillo  $\mathbb{Z}_{7681}$ , y tomando  $\phi = 1925$ , se puede calcular la transformada NTT  $\hat{g}$ . Aplicando luego la transformada inversa, es posible recuperar el vector original  $g$ .

$$\hat{g} = \begin{bmatrix} \phi^0 & \phi^1 & \phi^2 & \phi^3 \\ \phi^0 & \phi^3 & \phi^6 & \phi^1 \\ \phi^0 & \phi^5 & \phi^2 & \phi^7 \\ \phi^0 & \phi^7 & \phi^6 & \phi^5 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 1 & 1925 & 3383 & 6468 \\ 1 & 6468 & 4298 & 1925 \\ 1 & 5756 & 3383 & 1213 \\ 1 & 1213 & 4298 & 5756 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 2489 \\ 7489 \\ 6478 \\ 6607 \end{bmatrix} \quad (3.14)$$

Aplicando la transformada inversa, donde la inversa de  $\phi = 1925$  en  $\mathbb{Z}_{7681}$  es  $\phi^{-1} = 1213$  y el inverso del orden del polinomio  $n = 4$  es  $n^{-1} = 5761$ :

$$g = n^{-1} \begin{bmatrix} \phi^0 & \phi^0 & \phi^0 & \phi^0 \\ \phi^{-1} & \phi^{-3} & \phi^{-5} & \phi^{-7} \\ \phi^{-2} & \phi^{-6} & \phi^{-2} & \phi^{-6} \\ \phi^{-3} & \phi^{-1} & \phi^{-7} & \phi^{-5} \end{bmatrix} \cdot \hat{g} = 5761 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1213 & 5756 & 6468 & 1925 \\ 4298 & 3383 & 4298 & 3383 \\ 5756 & 1213 & 1925 & 6468 \end{bmatrix} \cdot \begin{bmatrix} 2489 \\ 7489 \\ 6478 \\ 6607 \end{bmatrix} \quad (3.15)$$

Con estas transformadas definidas se define el producto o convolución negativa en el anillo  $R_q := \frac{\mathbb{Z}_q[X]}{X^n + 1}$  entre dos polinomios  $g$  y  $h$  como:

$$g \cdot h = \text{NTT}^{-1}(\text{NTT}(g) \circ \text{NTT}(h)) \quad (3.16)$$

Donde la operación  $\circ$  denota la multiplicación elemento a elemento (o punto a punto) entre los vectores en  $\mathbb{Z}_q[X]$ .



Ahora, queda demostrar que el tiempo de ejecución de la NTT es de  $\mathcal{O}(n \log(n))$ . Para lograr este cometido, se aprovechan dos propiedades que cumplen estas raíces calculadas:

1. Peridicidad:

$$\phi^{k+2n} = \phi^k \quad (3.17)$$

2. Simetría:

$$\phi^{k+n} = \phi^{-k} \quad (3.18)$$

Con estas propiedades, se puede implementar el algoritmo de Cooley-Tukey [29] que consiste en ir descomponiendo el problema en mitades de manera recursiva para reducir al máximo la cantidad de cálculos realizados. Partiendo de la transformada directa y desarrollando:

$$\hat{a}_j = \sum_{i=0}^{n-1} \phi^{i(2j+1)} a_j \bmod q = \sum_{i=0}^{n/2-1} \phi^{4ij+2i} a_{2i} + \phi^{2j+1} \sum_{i=0}^{n/2-1} \phi^{4ij+2i} a_{2i+1} \bmod q \quad (3.19)$$

Si se sustituye  $A_j = \sum_{i=0}^{n/2-1} \phi^{4ij+2i} a_{2i}$  y  $B_j = \sum_{i=0}^{n/2-1} \phi^{4ij+2i} a_{2i+1}$ . Ahora aplicando simetría en  $\phi$ :

$$\hat{a}_j = A_j + \phi^{4ij+2i} B_j \bmod q \quad (3.20)$$

$$\hat{a}_{j+n/2} = A_j - \phi^{4ij+2i} B_j \bmod q \quad (3.21)$$

Donde las matrices  $A_j$  y  $B_j$  pueden obtenerse como el resultado de aplicar la NTT sobre la mitad de los puntos, gracias a la estructura recursiva del algoritmo. Esto implica que, si  $n$  es una potencia de 2, el proceso puede repetirse recursivamente sobre subproblemas de tamaño cada vez menor, hasta alcanzar el caso base.

De manera similar, se puede mostrar esta propiedad para la transformada inversa. Por tanto, se demuestra que este algoritmo tiene complejidad  $\mathcal{O}(n \log(n))$ .

En el caso concreto de Kyber [26], la Transformada (NTT) de un polinomio en el anillo  $R_q$  se representa como un vector de 128 polinomios de grado 1.

Sean las 256 raíces enésimas de la unidad  $\{\xi, \xi^3, \dots, \xi^{255}\}$ , con  $\xi = 17$  como primera raíz primitiva. Entonces, se cumple que:

$$X^{256} + 1 = \prod_{i=0}^{127} (X^2 - \xi^{2i+1}) \quad (3.22)$$

Aplicando la NTT propuesta en [26] a un polinomio  $f \in R_q$  se obtiene:

$$NTT(f) = \hat{f} = (\hat{f}_0 + \hat{f}_1 X, \hat{f}_2 + \hat{f}_3 X, \dots, \hat{f}_{254} + \hat{f}_{255} X) \quad (3.23)$$

Con

$$\begin{aligned} \hat{f}_{2i} &= \sum_{j=0}^{127} f_{2j} \xi^{(2i+1)j} \\ \hat{f}_{2i+1} &= \sum_{j=0}^{127} f_{2j+1} \xi^{(2i+1)j} \end{aligned} \quad (3.24)$$

Donde mediante la transformada directa NTT e inversa  $\text{NTT}^{-1}$  se puede realizar el producto de  $f, g \in R_q$  de manera eficiente de la siguiente manera:

$$h = f \cdot g = \text{NTT}^{-1} [\text{NTT}(f) \circ \text{NTT}(g)] \quad (3.25)$$

Siendo  $\hat{h} = \hat{f} \circ \hat{g} = \text{NTT}(f) \circ \text{NTT}(g)$  la multiplicación base definida como:

$$\hat{h}_{2i} + \hat{h}_{2i+1}X = (\hat{f}_{2i} + \hat{f}_{2i+1})(\hat{g}_{2i} + \hat{g}_{2i+1}) \bmod (X^2 - \xi^{2i+1}) \quad (3.26)$$

En la figura 3.5.1.1 se puede ver una representación gráfica de como funciona este proceso.

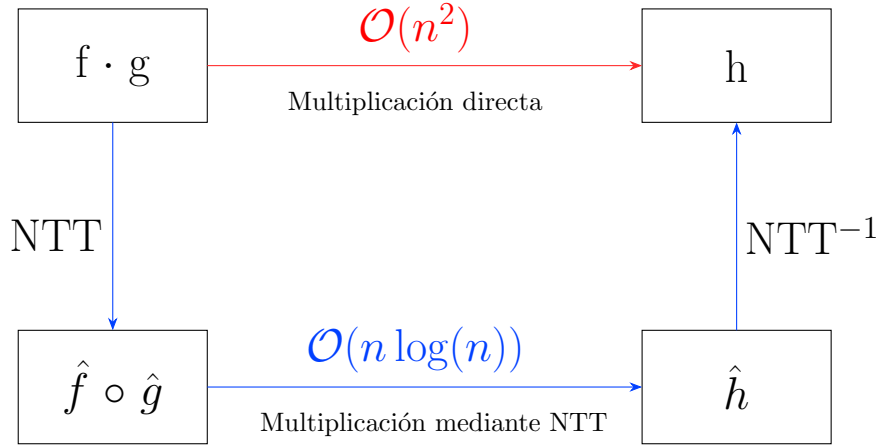


Figura 3.1: Representación del cálculo de un producto de polinomios mediante NTT en comparación con los algoritmos clásicos.

### 3.5.1.2. Aprendizaje Con Errores o Learning With Errors (LWE)

Para la elaboración de esta sección, se ha utilizado la información contenida en el artículo [30], el cual expone los fundamentos matemáticos del problema de Aprendizaje con Errores (Learning With Errors, LWE). Este problema constituye la base teórica sobre la que se sustenta el esquema criptográfico Kyber.

Para ello, los esquemas basados en LWE trabajan con un objeto matemático conocido como retícula. Una retícula es un conjunto discreto de puntos en el espacio, generado por todas las combinaciones lineales con coeficientes enteros de un conjunto de  $n$  vectores linealmente independientes que conforman una base  $\mathbb{B} = \{b_1, \dots, b_n\}$ :

$$\mathcal{A} = \mathcal{L}(\mathbb{B}) = \left\{ \sum_{i \in n} z_i b_i : z \in \mathbb{Z}^n \right\} \quad (3.27)$$

Esta definición será útil en la demostración de la seguridad de los esquemas basados en LWE. Aun así, antes de pasar a la explicación del algoritmo de intercambio de claves públicas, es necesario definir el problema de Aprendizaje con Errores.

El Aprendizaje con Errores consiste en la tarea de distinguir entre parejas de la forma  $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ , donde  $b_i \approx \langle a_i, s \rangle$ , y parejas generados de manera completamente aleatoria. Donde,  $s \in \mathbb{Z}_q^n$  es el secreto que se mantiene fijo para todas

las muestras,  $a_i \in \mathbb{Z}_q^n$  es un vector elegido uniformemente al azar, y  $\langle, \rangle$  denota el producto escalar Euclídeo.

La principal utilidad criptográfica del problema LWE radica en que, para quien no conoce el secreto, resulta computacionalmente difícil distinguir entre pares estructurados y pares aleatorios. En cambio, quien sí conoce el secreto puede identificar fácilmente qué parejas son consistentes con este, lo que permite construir esquemas seguros de cifrado e intercambio de claves.

### LWE en anillos

En Kyber no se parte del problema LWE “puro”, ya que los esquemas basados directamente en LWE suelen presentar claves de tamaño y tiempos de cálculo con un orden de magnitud  $\mathcal{O}(n^2)$  [31]. Esto se debe a que, al trabajar con matrices genéricas, se carece de la estructura de anillo necesaria para aprovechar multiplicaciones mediante convolución rápida, es decir, la NTT. En cambio, Kyber se fundamenta en una variante conocida como Ring-LWE, donde las operaciones de multiplicación matricial se pueden implementar como multiplicaciones de polinomios en  $\frac{\mathbb{Z}_q[x]}{X^n + 1}$ , lo cual permite usar la NTT.

En cuanto a la eficiencia en la reducción del tamaño de las claves, esta puede observarse claramente a través del siguiente ejemplo ilustrativo:

Esquema	LWE “puro”	Kyber (R-LWE)
Tamaño clave pública	$\mathcal{O}(n^2)$ bits	$\mathcal{O}(n)$
Operación para generar la pareja	$b_i = \langle a_i, s \rangle + e_i$	$b[x] = a[x] \cdot s[x] + e[x]$
Matriz $A$	$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$	$3+11X$
Secreto $s$	$\begin{pmatrix} 5 \\ 6 \end{pmatrix}$	$5+6X$
Error $e$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$1+X$
Resultado $b$	$\begin{pmatrix} 1 \\ 6 \end{pmatrix}$	$1+6X$

Tabla 3.1: Tabla con un ejemplo numérico del cálculo del valor  $b$  necesario para el problema LWE tanto en el caso puro como en la estructura de anillo de Kyber para ver como efectivamente en la clave pública  $(a, b)$  el tamaño es menor. En este ejemplo se trabaja en  $\mathbb{Z}_{17}$  y  $X^2 + 1$ .

Aunque la incorporación de estructura algebraica al problema criptográfico principal podría generar dudas sobre si se mantiene el mismo nivel de seguridad, esta cuestión se aborda en mayor detalle en la sección de seguridad, basándose en el artículo [30]. Allí se explica cómo R-LWE ofrece garantías criptográficas equivalentes a las del LWE original, por lo que este cambio no supone una debilidad, sino una optimización con respaldo teórico.

### Aplicación del R-LWE para el intercambio de claves públicas

A continuación, se presenta el algoritmo principal empleado para el intercambio de claves basado en el problema R-LWE que fundamenta matemáticamente el funcionamiento de Kyber.

---

**Algoritmo 1** Generación claves R-LWE en  $\mathbb{Z}_q[x]/(X^n + 1)$

---

**Entrada:**  $q, n$

---

**Salida:**  $sk, pk$

---

1: 1

---



---

**Algoritmo 2** Cifrado R-LWE

---

**Entrada:**  $pk, z$

---

**Salida:**  $u, v$

---

1: 1

---



---

**Algoritmo 3** Descifrado R-LWE

---

**Entrada:**  $sk, u, v$

---

**Salida:**  $z$

---

1: 1

---

#### 3.5.1.3. Fundamentos de seguridad de Kyber

Seguridad basada en retículas ideales

Seguridad esperada

Análisis respecto a ataques conocidos

#### 3.5.1.4. Algoritmos principales

#### 3.5.2. SABER

Para [32]

#### 3.5.3. Hamming Quasi-Cyclic (HQC)

Para [33]

#### 3.5.4. Bit Flipping Key Encapsulation (Bike)

Para [34]

# Capítulo 4

## Desarrollo

### 4.1. Implementación comunicación serie

#### 4.1.1. Parámetros generales y formato mensajes

#### 4.1.2. Implementación en el ordenador

#### 4.1.3. Implementación en el microprocesador

### 4.2. Estructura y API para los algoritmos de cifrado asimétrico

#### 4.2.1. Kyber

#### 4.2.2. Saber

#### 4.2.3. Bike

#### 4.2.4. HQC

### 4.3. Implementación algoritmos en el PC

#### 4.3.1. Compilación en librerías

#### 4.3.2. Diagrama de uso

#### 4.3.3. Diagrama funcional

#### 4.3.4. Diagrama de clases

### 4.4. Implementación de algoritmos en el microcontrolador

#### 4.4.1. Diagrama de uso

#### 4.4.2. Diagrama funcional

### 4.5. Implementación del intercambio de claves. Creación del secreto compartido

Hablar de los modelos de comunicaciones a implementar .... (msg teams)

**4.5.1. Modelo 1**

**4.5.2. Modelo 2**

**4.5.3. Modelo 3**

**4.6. Tests de rendimiento realizados**

# Capítulo 5

## Resultados y discusión

En este capítulo se muestran los resultados obtenidos de aplicar las rutinas desarrolladas con anterioridad.

### 5.1. Resultados

#### 5.1.1. (No sé si lo metere) Resultado de ejecución de los algoritmos clásicos

##### 5.1.1.1. RSA

##### 5.1.1.2. ECC

#### 5.1.2. Resultados de ejecución de los algoritmos post-cuánticos

##### 5.1.2.1. Kyber

##### 5.1.2.2. Saber

##### 5.1.2.3. HQC

##### 5.1.2.4. Bike

#### 5.1.3. Resultados de los distintos modelos de comunicación

##### 5.1.3.1. Modelo 1

##### 5.1.3.2. Modelo 2

##### 5.1.3.3. Modelo 3

### 5.2. Discusión

#### 5.2.1. Comparativa entre los distintos algoritmos post-cuánticos analizados

#### 5.2.2. Comparativa entre los distintos modelos de comunicación





## Capítulo 6

# Conclusiones

Se presentan a continuación las conclusiones del proyecto y desarrollos futuros para mejorar la implementación.

### 6.1. Conclusión

Una vez finalizado el proyecto...

### 6.2. Desarrollos futuros

Un posible desarrollo...



# Bibliografía

- [1] Leslie Lamport et al. The latex project, 2024.
- [2] Tikzmaker. <https://tikzmaker.com/editor>, 2024.
- [3] ISO/IEC 9899:2018 Information technology ? Programming languages ? C. <https://www.iso.org/standard/82075.html>, 2024. International Organization for Standardization, Geneva, Switzerland.
- [4] ISO/IEC 14882:2025 Information technology ? Programming languages ? C++. <https://www.iso.org/standard/83626.html>, 2024. International Organization for Standardization, Geneva, Switzerland.
- [5] Infineon Technologies AG. CY8CPROTO-063-BLE PSoC 6 BLE Prototyping Kit. <https://www.infineon.com/cms/en/product/evaluation-boards/cy8cproto-063-ble/>, 2020. Consultado: 2025-05-05.
- [6] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Yi-Kai Liu. Status report on the third round of the nist post-quantum cryptography standardization process. NIST Interagency Report NIST IR 8413 (Updated), National Institute of Standards and Technology (NIST), July 2022.
- [7] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, and Noah Waller. Status report on the fourth round of the nist post-quantum cryptography standardization process. NIST Internal Report NIST IR 8545, National Institute of Standards and Technology (NIST), Gaithersburg, MD, March 2025.
- [8] Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu, and Hong Guo. Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 11(1):011318, 03 2024.
- [9] Mandeep Kumar and Bhaskar Mondal. A brief review on quantum key distribution protocols. *Multimedia Tools and Applications*, January 2025.
- [10] Akoh Atadoga, Oluwatoyin Ajoke Farayola, Benjamin Samson Ayinla, Olukunle Oladipupo Amoo, Temitayo Oluwaseun Abrahams, and Femi Osasona. A comparative review of data encryption methods in the usa and europe. 5:447–460, Feb. 2024.

- [11] Qixin Zhang. An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. In *2021 2nd International Conference on Computing and Data Science (CDS)*, pages 616–622, 2021.
- [12] Basel Halak, Yildiran Yilmaz, and Daniel Shiu. Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications. *IEEE Access*, 10:76707–76719, 2022.
- [13] Mila Anastasova, Panos Kampanakis, and Jake Massimo. PQ-HPKE: Post-quantum hybrid public key encryption. Cryptology ePrint Archive, Paper 2022/414, 2022.
- [14] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, and C. N. Asogwa. An overview of quantum cryptography and shor’s algorithm. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(5):7487–7495, September 2020.
- [15] David Aasen, Morteza Aghaee, Zulfi Alam, and Mariusz Andrzejczuk et al. Roadmap to fault tolerant quantum computation using topological qubit arrays, 2025.
- [16] Fouzia Samiullah, Ming-Lee Gan, Sedat Akleylek, and Y. Aun. Quantum resistance saber-based group key exchange protocol for iot. *IEEE Open Journal of the Communications Society*, 6:378–398, 2025.
- [17] National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication FIPS 203, National Institute of Standards and Technology, Gaithersburg, MD, USA, August 2024.
- [18] National Institute of Standards, Technology (NIST), and Morris J. Dworin. Sha-3 standard: Permutation-based hash and extendable-output functions, 2015-08-04 00:08:00 2015.
- [19] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.
- [20] John Proos and Christof Zalka. Shor’s discrete logarithm quantum algorithm for elliptic curves, 2004.
- [21] Siyon Singh and Eric Sakk. Implementation and analysis of shor’s algorithm to break rsa cryptosystem security. January 2024.
- [22] Gorjan Alagic, Elaine Barker, Lily Chen, Dustin Moody, Angela Robinson, Hamilton Silberg, and Noah Waller. Recommendations for key-encapsulation mechanisms: Initial public draft. NIST Special Publication NIST SP 800-227 ipd, National Institute of Standards and Technology (NIST), January 2025.
- [23] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO’ 99*, volume 1666 of *Lecture Notes in Computer Science*, pages 537–554, Berlin, Heidelberg, 1999. Springer.

- [24] National Institute of Standards and Technology. Post-quantum cryptography - round 3 submissions. <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions>, 2020. Consultado: 2025-05-05.
- [25] National Institute of Standards and Technology. Post-quantum cryptography - round 4 submissions. <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions>, 2022. Consultado: 2025-05-05.
- [26] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation (version 3.01). Technical report, CRYSTALS Project, January 2021. NIST PQC Round 3 submission.
- [27] Ardianto Satriawan, Rella Mareta, and Hanho Lee. A complete beginner guide to the number theoretic transform (NTT). Cryptology ePrint Archive, Paper 2024/585, 2024.
- [28] Miguel A. Moreno. Primitive  $n$ -th roots of unity of finite fields. <https://www.csd.uwo.ca/~mmorenom/CS874/Lectures/Newton2Hensel.html/node9.html>, n.d. Consultado: 2025-05-05.
- [29] James W. Cooley and John W. Tukey. An algorithm for the machine calculation of complex fourier series. *Mathematics of Computation*, 19(90):297–301, 1965.
- [30] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6), November 2013.
- [31] Daniele Micciancio and Oded Regev. *Lattice-based Cryptography*, pages 147–191. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
- [32] Andrea Basso, José María Bermudo Mera, Jan-Pieter D’Anvers, Angshuman Karmakar, Sujoy Sinha Roy, Michiel Van Beirendonck, and Frederik Vercauteren. SABER: Mod-LWR based KEM (Round 3 Submission). Technical report, Katholieke Universiteit Leuven and University of Birmingham, 2020. NIST PQC Round 3 submission.
- [33] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jurjen Bos, Jean-Christophe Deneuville, Arnaud Dion, Philippe Gaborit, Jérôme Lacan, Edoardo Persichetti, Jean-Marc Robert, Pascal Véron, and Gilles Zémor. HQC: Hamming Quasi-Cyclic (Fourth Round Submission). Technical report, HQC Team, October 2022. NIST PQC Round 4 submission.
- [34] Nicolas Aragon, Paulo S. L. M. Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Santosh Ghosh, Shay Gueron, Tim Güneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Jan Richter-Brockmann, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, and Gilles Zémor. BIKE: Bit Flipping Key Encapsulation (Round 4 Submission). Technical report, BIKE Team, October 2022. NIST PQC Round 4 submission.