UNIVERSIDAD
DE GRANADA

Facultad de Ciencias y Escuela Técnica Superior de Ingenierías
Informática y Telecomunicación

Doble Grado en Matemáticas e Ingeniería Informática

TRABAJO DE FIN DE GRADO

Criptografía basada en retículos

Presentado por:
Mario Rodríguez López

Curso académico 2024-2025

Criptografía basada en retículos

Mario Rodríguez López

Mario Rodríguez López *Criptografía basada en retículos* .
Trabajo de fin de Grado. Curso académico 2024-2025.

Responsable de tutorización

Francisco Javier Lobillo Borrero
Departamento de Álgebra

Nombre del tutor 2
Departamento del tutor 2

Doble Grado en Matemáticas e Ingeniería Informática

Facultad de Ciencias y Escuela Técnica Superior de Ingenierías Informática y Telecomunicación

Universidad de Granada

Declaración de originalidad

D./Dña. Mario Rodríguez López

Declaro explícitamente que el trabajo presentado como Trabajo de Fin de Grado (TFG), correspondiente al curso académico 2024-2025, es original, entendido esto en el sentido de que no he utilizado para la elaboración del trabajo fuentes sin citarlas debidamente.

En Granada a 1 de diciembre de 2024

Fdo: Mario Rodríguez López

A mis padres, por apoyarme siempre

Índice general

Agradecimientos

Agradecimientos (opcional, ver archivo `preliminares/agradecimiento.tex`).

Summary

An english summary of the project (around 800 and 1500 words are recommended).
File: `preliminares/summary.tex`

Resúmen

De acuerdo con la comisión de grado, el TFG debe incluir una introducción en la que se describan claramente los objetivos previstos inicialmente en la propuesta de TFG, indicando si han sido o no alcanzados, los antecedentes importantes para el desarrollo, los resultados obtenidos, en su caso y las principales fuentes consultadas.

Ver archivo `preliminares/introduccion.tex`

Motivación

Vivimos en una era donde la digitalización ha transformado todos los aspectos de nuestra vida cotidiana. Desde la forma en que nos comunicamos, hasta cómo almacenamos información y accedemos a servicios esenciales, la dependencia de las tecnologías digitales es innegable. Esta digitalización, aunque ofrece innumerables beneficios en términos de eficiencia y conveniencia, también presenta desafíos significativos en cuanto a la protección de la información y la privacidad. Aquí es donde entra en juego la criptografía.

La criptografía es esencial en nuestra vida diaria, aunque muchas veces pase desapercibida. Su importancia radica en la capacidad de proteger la información confidencial, garantizar la privacidad y asegurar la integridad de los datos en un mundo cada vez más digitalizado. Desde el uso de tarjetas de crédito y transacciones bancarias en línea hasta la comunicación a través de aplicaciones de mensajería y el almacenamiento de datos personales en la nube, la criptografía asegura que estos procesos sean seguros y que la información no caiga en manos equivocadas.

Con el avance imparable de la tecnología, nos enfrentamos a una amenaza que desafía la seguridad de los métodos criptográficos tradicionales: la computación cuántica.

Actualmente, los algoritmos criptográficos más utilizados, como RSA y ECC (Criptografía de Curva Elíptica), se basan en problemas matemáticos complejos, como la factorización de números enteros grandes y el logaritmo discreto, que son extremadamente difíciles de resolver con la computación clásica. Sin embargo, estos problemas pueden ser resueltos de manera eficiente por los ordenadores cuánticos utilizando el algoritmo de Shor.

El algoritmo de Shor, desarrollado por el matemático Peter Shor en 1994, es capaz de factorizar números enteros grandes y resolver problemas de logaritmos discretos en un tiempo significativamente menor que los algoritmos clásicos. Esto implica que los ordenadores cuánticos podrían romper la mayoría de los sistemas criptográficos actuales, exponiendo información confidencial y comprometiendo la seguridad de los datos.

En este contexto, surge la necesidad urgente de desarrollar y adoptar sistemas criptográficos que sean resistentes a los ataques de la computación cuántica. Aquí es donde entra en juego el criptosistema post-cuántico Kyber-Crystals, una de las propuestas más prometedoras en el ámbito de la criptografía post-cuántica y el que fue seleccionado como el nuevo estándar de criptografía por el National Institute of Standards and Technology (NIST) en el año 2022, un reconocimiento que subraya su importancia y robustez frente a las amenazas cuánticas.

Kyber-Crystals se basa en problemas matemáticos en retículos o redes, que son considerados intratables incluso para los ordenadores cuánticos. Este enfoque garantiza que los datos cifrados bajo este sistema permanezcan seguros, resistiendo tanto a los ataques tradicionales como a los potenciales ataques cuánticos. La adopción de Kyber-Crystals como estándar de

criptografía por el NIST es un hito significativo, ya que refleja una confianza institucional en su capacidad para proteger la información en un futuro dominado por la tecnología cuántica.

Parte I.

Fundamento Teórico. Reticulos, MDLW & Crystals-Kyber

1. Preliminares

1.1. Definición

Un retículo en $\mathbb{R}^n$ es un subgrupo aditivo discreto de $\mathbb{R}^n$ definido como el conjunto de todas las combinaciones lineales enteras de n vectores linealmente independientes. Este conjunto de vectores se conoce como una base del retículo y no es único. Es decir un reticulo es el conjunto de todas las combinaciones lineales enteras de vectores de una base $B = \{b_1, b_2, \ldots, b_n\} \subset \mathbb{R}^n$.

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z} \right\}$$

2. Teoría de Reticulos

2.1. Definición

Un retículo en $\mathbb{R}^n$ es un subgrupo aditivo discreto de $\mathbb{R}^n$ definido como el conjunto de todas las combinaciones lineales enteras de n vectores linealmente independientes. Este conjunto de vectores se conoce como una base del retículo y no es único. Es decir un reticulo es el conjunto de todas las combinaciones lineales enteras de vectores de una base $B = \{b_1, b_2, \ldots, b_n\} \subset \mathbb{R}^n$.

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z} \right\}$$

3. Problemas en reticulos y criptografia basada en reticulos

3.1. Problemas en reticulos y criptografia basada en reticulos

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

4. LWE, Ring-LWE, Module-LWE

4.1. Primera sección

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

5. Crystals-Kyber funcionamiento y dureza.

5.1. Primera sección

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

6. Posibles ataques a Crystals-kyber.

6.1. Primera sección

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

7. Complejidad del desencriptado

7.1. Primera sección

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

Parte II.

Implementaciones realizadas. Metodologia usada para el desarrollo y codigo implementado

8. KANBAN y toma de decisiones

8.1. Primera sección

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

9. Implementación del criptosistema

9.1. Primera sección

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

10. Ataque a crystals-kyber

10.1. Primera sección

Este fichero `capitulo-ejemplo.tex` es una plantilla para añadir capítulos al TFG. Para ello, es necesario:

- Crear una copia de este fichero `capitulo-ejemplo.tex` en la carpeta `capitulos` con un nombre apropiado (p.e. `capitulo01.tex`).
- Añadir el comando `\input{capitulos/capitulo01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho capítulo.

A. Ejemplo de apéndice

Los apéndices son opcionales.

Este fichero `apendice-ejemplo.tex` es una plantilla para añadir apéndices al TFG. Para ello, es necesario:

- Crear una copia de este fichero `apendice-ejemplo.tex` en la carpeta `apendices` con un nombre apropiado (p.e. `apendice01.tex`).
- Añadir el comando `\input{apendices/apendice01}` en el fichero principal `tfg.tex` donde queremos que aparezca dicho apéndice (debe de ser después del comando `\appendix`).

Glosario

La inclusión de un glosario es opcional.
Archivo: `glosario.tex`

$\mathbb{R}$ Conjunto de números reales.

$\mathbb{C}$ Conjunto de números complejos.

$\mathbb{Z}$ Conjunto de números enteros.