UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

Propuesta TFG. Curso 2025/2026

GRADO: Grado en Matemáticas

CÓDIGO DEL TFG: 270-024-2025/2026

1. DATOS BÁSICOS DEL TFG:

Título: El criptosistema BIKE

Descripción general (resumen y metodología):

La publicación del algoritmo de Shor en 1994 demostró la vulnerabilidad de los actuales criptosistemas de clave pública ante el eventual desarrollo de ordenadores cuánticos. Para cubrir la eventual ruptura de RSA y los criptosistemas basados en la estructura de grupo de una curva elíptica, el NIST (National Institute of Standards and Technology) lanzó en Enero de 2017 un concurso para reemplazarlos por criptosistemas resistentes a ataques realizados por ordenadores cuánticos. La comunidad criptográfica optó por el desarrollo de criptosistemas basados en problemas de decisión NP-completos. Uno de dichos problemas es la decodificación de un código lineal binario arbitrario. En 1978 McEliece propone un criptosistema basado en la dificultad de encontrar una decodificación eficiente en general. En su propuesta utiliza los códigos Goppa. En los últimos años numerosas variantes han sido propuestas reemplazando los códigos Goppa por otras familias con algoritmos de decodificación eficientes. Uno de los algoritmos que ha alcanzado la cuarta y última ronda del concurso propuesto por el NIST es el BIKE, un ejemplo de criptografía basada en códigos que utiliza como familia de códigos los QC-MDPC (Quasi-Cyclic Moderate Density Parity-Check). En este Trabajo de Fin de Grado se estudiará dicho criptosistema.

Tipología: Estudio de casos, teóricos o prácticos, relacionados con la temática del Grado.

Objetivos planteados:

- Conocer los elementos básicos de la criptografía basada en códigos.
- Describir los códigos QC-MDPC y sus algoritmos de decodificación.
- Describir el criptosistema BIKE.
- Describir el IND-CCA2 KEM asociado.

Bibliografía básica:

1. Nicolas Aragon, et al. BIKE: Bit Flipping Key Encapsulation. Specification Document. https://bikesuite.org/files/v5.2/BIKE_Spec.2024.10.10.1.pdf 2024/10/10.
2. R. Misoczki, J. -P. Tillich, N. Sendrier and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes," 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, 2013, pp. 2069-2073, doi: 10.1109/ISIT.2013.6620590.

Recomendaciones y orientaciones para el estudiante:

Plazas: 1

2. DATOS DEL TUTOR/A:

Nombre y apellidos: FRANCISCO JAVIER LOBILLO BORRERO

Ámbito de conocimiento/Departamento: ÁLGEBRA

Correo electrónico: jlobillo@ugr.es

3. COTUTOR/A DE LA UGR (en su caso):

Nombre y apellidos:

Ámbito de conocimiento/Departamento:

Correo electrónico:

4. COTUTOR/A EXTERNO/A (en su caso):

Nombre y apellidos:

Correo electrónico:

Nombre de la empresa o institución:

Dirección postal:

Puesto del tutor en la empresa o institución:

Centro de convenio Externo:

5. DATOS DEL ESTUDIANTE:

Nombre y apellidos: DANIEL PRADOS SERRANO

Correo electrónico: danips04@correo.ugr.es