Identificación del proyecto

Nombre del proyecto

Retos en Códigos Algebraicos y en Criptografía basada en la Teoría de la Información para un entorno de comunicaciones digitales

Expediente numero

PID2021-124928NB-I00

Descripción del proyecto

Este proyecto está dedicado al estudio de dos objetos matemáticos pertenecientes a la Teoría de Códigos y la Criptografía, respectivamente: los códigos algebraico-geométricos (AG) y los esquemas de compartición de secretos. Aunque estos objetos están, en general, orientados a distintas finalidades, comparten sus raíces teóricas. En este proyecto estudiaremos problemas abiertos fundamentales sobre códigos AG y esquemas de compartición de secretos, así como aspectos computacionales que afectan sus aplicaciones prácticas. En particular trabajaremos en problemas relacionados con la Teoría de Matroides y con los semigrupos numéricos. Los principales problemas que consideramos son los siguientes: 1) Construir códigos cuánticos a partir de secuencias anidadas de códigos 2) Mejorar las construcciones de esquemas de compartición de secretos, con especial énfasis en aquellos esquemas que se utilizan como primitiva en protocolos de computación multiparte seguros, y aquellos con estructuras de acceso interesantes. Queremos conocer las limitaciones de esta primitiva criptográfica obteniendo cotas inferiores en el tamaño de los fragmentos 3) Desarrollar nuevas técnicas para la caracterización de matroides lineales, multilineales, algebraicos o entrópicos 4) Analizar el comportamiento asintótico de semigrupos numéricos. Además, hay una parte del proyecto que está dedicada a la ejecución eficiente de los algoritmos de codificación y decodificación. Esta parte está orientada a la aceleración de esquemas criptográficos post-cuánticos (PQ) que se basan en códigos lineales. Estas contribuciones se extenderán a esquemas PQ basados en retículos y a códigos lineales en general.

Financiación

Entidad financiadora

MCIN/ AEI /10.13039/501100011033/ y por FEDER Una manera de hacer Europa

Importe

174.240,00 €