Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 8 de abril de 2025, 15:00 horas (GMT+1)

Products of codes and cryptanalysis in code-based cryptography

Rocco Mora
CISPA Helmholtz-Zentrum für Informations[1]

This talk explores the use of the component-wise product of spaces in the analysis of cryptosystems based on linear error-correcting codes. One of the main applications is the structural cryptanalysis of McEliece-like schemes. After recalling the motivations and the necessary tools, we will review recent advances in distinguishing families of algebraic codes from random ones and recovering their secret keys using the square-code approach within the McEliece framework. We highlight the strengths of these techniques and discuss strategies to possibly overcome their limitations. We will also mention how the product of codes construction and its possible generalizations can be effectively leveraged to address another computational problem used in code-based cryptography, namely the code equivalence problem.

[1]CISPA Helmholtz-Zentrum für Informations
Saarbrücken
Alemania
rocco.mora@cispa.de