CIDMA CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

Systems and Control Group Seminar

10 November, 2023, 11:00

Mathematics Department, University of Aveiro

Room Sousa Pinto (11.2.6)

A convolutional approach to the McEliece cryptosystem with binary Goppa codes

Miguel Beltrá Vidal

University of Alicante, Spain

miguel.beltra@ua.es

Abstract

The McEliece cryptosystem is a public key cryptosystem for which no attack using a quantum computer is known, and therefore is a promising candidate for the Post-quantum Cryptography. Its main drawback is the large public key it uses, which is a consequence of the underlying block Goppa codes. In this talk we show how to reduce the size of the public key using a convolutional mask.

This seminar was supported in part by the Portuguese Foundation for Science and Technology (FCT – Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UIDB/04106/2020.

fct Fundação para a Ciência e a Tecnologia

REPÚBLICA PORTUGUESA