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

Seminar
Systems and Control Group - CIDMA

20 de novembro de 2019, 16h00

Departamento de Matemática, Universidade de Aveiro
Sala 11.2.16

A McEliece-type cryptosystem based on convolutional codes

Diego Napp

Universidade de Alicante
diegonapp@gmail.com

Abstract

The McEliece cryptosystem is the 1rst post-quantum system based on algebraic coding theory. Its security is based on the hard problem of decoding a random linear code. First attempts to use convolutional codes in this cryptosystem have been recently proposed. However, these schemes consider fixed block lengths (with the block Toeplitz structure typical of convolutional codes) and therefore had many similarities with block codes. In this paper, we investigate further the possibility of using convolutional codes instead of block codes.

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 UID/MAT/04106/2019.

FCT Fundação para a Ciência e a Tecnologia