## The Code Equivalence Problem: signatures, attacks and other adventures

Paolo Santini (Università Politecnica delle Marche)

Abstract: The Code Equivalence Problem (CEP) asks to find a linear isometry (a monomial or a permutation) mapping a given code into another given code. The problem can be phrased in terms of group actions and, as such, yields a natural mean to build digital signatures (via Fiat-Shamir transforming of a Sigma protocol). Despite being a rather old problem, its use in cryptography is quite recent. Consequently, there are many open problems and research questions related to CEP. In this talk we provide an overview of the most important features of CEP, with a special focus on recent results and open questions.