Algebraic Cryptanalysis in codebased and multivariate cryptography

Magali Bardet

Abstract

Algebraic cryptanalysis has become unavoidable in the cryptanalysis and design of schemes in cryptography. In a first part, I will explain what is a good algebraic modeling, and how we can estimate the complexity of solving a polynomial system with Gröbner basis. In the second part, I will present different algebraic modelings for the decoding problem in rank metric code-based cryptography, and their complexity analysis.