Bernoullis Tafelrunde

Graduate Student Seminar

Monday, March 21 2022, 12:15-13:00
Hybrid seminar
Seminar room 05.002, Spiegelgasse 1 / Zoom

Giulia Gaggero

Université de Neuchâtel

Multivariate Cryptography

Abstract

In this talk I will give an outlook of what multivariate cryptography is. First of all we look at the concept of digital signature. Then we recall some algebraic tools, further we look at the main invariants that are used in the crypto-analysis of a multivariate digital signature scheme. Given a system in a polynomial ring with n variables over a field K, we introduce the solving degree of the system and, in order to estimate it, we look at the Castelnuovo-Mumford regularity of the ideal generated by the homogenized system, the last fall degree and the degree of regularity of the system.