Multivariate cryptography and the hardness of polynomial system solving

Elisa Gorla (Universities of Neuchatel)

Abstract: Multivariate cryptography belongs to post-quantum cryptography, which is the branch of cryptography which remains secure even in the presence of a quantum computer. After introducing motivating the need for post-quantum cryptography, I will discuss the role played by commutative algebra techniques in multivariate cryptography. The security of multivariate cryptographic primitives relies on the hardness of computing the solutions of multivariate polynomial systems over finite fields. Since we can compute the solutions of a polynomial system from its Groebner basis, bounds on the complexity of Groebner bases computations provide bounds on the security of the corresponding multivariate cryptographic primitives. In this talk, I will introduce and discuss some algebraic invariants which play a role in these security estimates and motivate their importance in this applied setting.