SEMINARIO

Elisa Gorla

University of Neuchâtel, Switzerland

Multivariate cryptography and the complexity of solving random polynomial systems

Abstract:

The study of the complexity of solving a system of polynomial equations over a finite field is a central problem in symbolic computation, with a wide range of applications. In this talk, we focus on the applications to post-quantum cryptography, more specifically to multivariate cryptography. In multivariate cryptography, the security of the cryptosystem relies on the computational hardness of finding the solutions of a system of polynomial equations over a finite field. Therefore, estimating the complexity of solving a given system of polynomial equations produces an estimate for the security of the corresponding cryptosystem. Often, in their analysis, cryptographers make the assumption that the systems that they analyze are "random". In this talk, we discuss two distinct mathematical formulations for randomness of a system of equations. For each of them, we show estimates on the complexity of system solving by means of Groebner bases techniques. The new results that we present are joint work with M. Bigdeli, E. De Negri, M. Dizdarevic, R. Minko, and S. Tsakou.

El seminario tendrá lugar en Webex:
Número de reunión: 137 462 0171
https://profevirtual.webex.com/profevirtual/j.php?MTID=m6d09a303029cac2b557d3c6c81435447

Para participar y recibir la contraseña de la reunión se necesita registro:
https://forms.gle/sYzJW1uEdCtef4VX8

Webex (número de reunión 137 462 0171)
Martes 6 de Octubre de 2020 (16:00)
Organiza: GIR SINGACOM