IMUB | Institut de Matemàtica

Advanced Course

Polynomial systems in post-quantum cryptography

12 de març de 2024
19 de març de 2024

2 d'abril de 2024
9 d'abril de 2024
16 d'abril de 2024

Alessio Caminata
Università degli Studi di Genova

The main goal of this course is to give an introduction to the main areas of post-quantum cryptography and explain how multivariate polynomial systems play a key role in many of them. The course is organized as follows: In the first part, we will briefly recall the classical mathematical problems for public-key cryptography (factoring integers and discrete logarithm problem), and we will give an introduction to the main alternatives in post-quantum cryptography (multivariate, isogeny-based, code-based, and lattice-based). In the second part, we will focus on multivariate cryptography and the algebraic attack. We will introduce the linear-algebra-based algorithms for polynomial system solving and the notion of solving degree. Finally, we will present the connection of the solving degree with other invariants such as the degree of regularity, last fall degree, and Castelnuovo-Mumford regularity. The target audience includes master's students, graduates, and faculty staff. No prior knowledge in cryptography is required.

Lloc: Aula IMUB
Hora: 11-13h

www.imub.ub.edu

UNIVERSITAT DE BARCELONA