Instituto Universitario de Investigación de Matemáticas y Aplicaciones Universidad Zaragoza

Departamento de Matemáticas Universidad Zaragoza

Facultad de Ciencias Universidad Zaragoza

Seminario de Doctorandos Rubio de Francia

Conferencia

por

Pilar Coscojuela

Universidad Complutense de Madrid

Título:

Multivariate cryptography: seeking post-quantum alternatives to current cryptography

Resumen:

The security of today's public-key cryptography relies mainly on two problems: integer factorization and the computation of discrete logarithms over a cyclic group of large order. From a computational point of view, both are characterized by being easy to compute an instance of these problems from initial data but infeasible for a conventional computer to recover this data from the result. Since all known classical algorithms to solve these problems have exponential complexity in the size of the input, if we choose sufficiently large keys, encryption and digital signature schemes based on them will have the desired properties.

A landmark was Shor's algorithm in 1994, which allows solving these problems in polynomial time if we have a quantum computer. The question now is, can we build quantum computers large enough to pose a threat to today's cryptography?

The remarkable strides in its development in recent years have sparked growing interest in designing new cryptosystems whose security is not contingent on the creation of such computers.

In this talk, after an introduction to basic concepts, we will focus on multivariable cryptography, which comprises a set of post-quantum schemes based on the NP-hardness of the "MQ Problem". We will explain how and why Groebner bases are useful for studying its security, using a specific example of a multivariable cryptosystem, the DME.

Fecha: Jueves, 21 de marzo de 2024.
Hora: 17:00 horas.
Lugar: Seminario Rubio de Francia. Primera planta, Edificio B, Facultad de Ciencias.