Instituto Universitario de Investigación de Matemáticas y Aplicaciones Universidad Zaragoza
Departamento de Matemáticas Universidad Zaragoza
Facultad de Ciencias Universidad Zaragoza

Seminario Rubio de Francia

Conferencia

por

Miguel Ángel Marco Buzunáriz
Universidad de Zaragoza

Título:

Demostraciones en conocimiento cero.

Resumen: Las demostraciones en conocimiento cero son protocolos criptográficos entre dos partes, en los que una de ellas convence a la otra de la veracidad de una cierta afirmación, sin revelar información sobre las razones por las que dicha afirmación es cierta. Aunque pueda parecer contrario a la experiencia matemática habitual, estos protocolos existen para una familia muy amplia de afirmaciones (siendo precisos, para cualquier lenguaje en la clase NP), aunque están sujetos a ciertas limitaciones.

En esta charla daremos una visión general de esta teoría, y mostraremos con más detalle el ejemplo del protocolo Pinocho. Este protocolo usa pairings de curvas elípticas para generar pruebas (que consisten únicamente en ocho puntos de la curva) de cualquier afirmación NP.

Fecha: Jueves, 17 de Noviembre de 2022.
Hora: 12:00 horas.
Lugar: Seminario Rubio de Francia. Primera planta, Edificio B, Facultad de Ciencias.
Web: `http://anamat.unizar.es/seminario.html`