SIMBa

BGSMath
BARCELONA GRADUATE SCHOOL OF MATHEMATICS

Seminari Informal de Matemàtiques de Barcelona

***Speaker*:** Marta Bellés Muñoz.
University: Universitat Pompeu Fabra.

Date: Wednesday, December 15th, 2021.
Schedule: 12:00, *virtual coffee break*; 12:20, talk.
Place: Zoom (the link will be posted on our website).
Language: English.

Title: On Zero-Knowledge Proofs

Abstract: Informally speaking, zero-knowledge protocols are cryptographic tools that allow you to prove that you know a secret without revealing it. More precisely, a zero-knowledge proof allows one party to convince another that a statement is true without revealing anything other than the veracity of the statement. This type of proofs were introduced in 1989 as theoretical cryptographic objects, but the appealing properties of the protocols have made them become crucial tools in many real-world applications with strong privacy issues. In this presentation I will explain the main ideas behind zero-knowledge, I will talk about the type of statements that we know can be proved with zero-knowledge, and present some of the most outstanding applications of this technology.

About us: *SIMBa* is a youth mathematics seminar organized by graduate students in the Barcelona area. It is aimed towards graduate and last course undergraduate students. Our goals are divulging the knoweledge from different branches of mathematics for those interested and promote networking between the attendants.
This seminar is backed by the Faculty of Mathematics and Computer Science at Universitat de Barcelona, Faculty of Mathematics and Statistics at Universitat Politècnica de Catalunya, the Department of Mathematics from Univesitat Autònoma de Barcelona, CRM, IMUB and BGSMath.

Fore more information, visit at `www.ub.edu/simba/en/`.

If you have any doubt or comment do not hesitate to contact us by sending an email to ***seminari.simba@gmail.com***.