SIMBa
Seminari Informal
de Matemàtiques de Barcelona

UNIVERSITAT DE BARCELONA

B:KC Barcelona Knowledge Campus

Seminari Informal de Matemàtiques de Barcelona

***Speaker*:** Enric Florit Zacarías.
University: Universitat de Barcelona.

Date: Wednesday, 27th of November.
Schedule: 12:00, *coffee break*; 12:20, talk.
Place: B1 classroom, *Facultat de Matemàtiques* of UB.
Language: English.

Title: Postquantum cryptography: what, why, and how?

Abstract: The key agreement scheme proposed by Diffie and Hellman in 1976 relies on the problem of finding discrete logarithms. One can choose appropriate groups where the best algorithms for solving this problem are too slow, such as certain elliptic curves over finite fields. There are already proposed quantum algorithms that break discrete logarithms in polynomial time. For this reason multiple "post-quantum" cryptography primitives have appeared in the last years, while trying to find harder computational problems. One of the proposed protocols using elliptic curves is SIDH/SIKE, candidate to the NIST Post-Quantum Cryptography Competition.

About us: The SIMBa is a young seminar organized by the PhD students of the Faculties of Mathematics and Computers of Barcelona. It is aimed at doctoral, master's degree students and, also, for those who are in the last grade courses. Our goal is that each one can make known the research which they are doing, as well as, to get new knowledge of other areas of mathematics than his own..

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@ub.edu***.