Contribution ID: **49** Type: **Contributed Talk**

On homomorphic encryption using abelian groups

Friday, 27 February 2026 10:10 (20 minutes)

In this talk, we will look at the public key encryption scheme suggested by Leonardi and Luiz-Ropez that is based on the hardness of the learning homomorphism with noise problem (this is a generalisation of the learning with errors (LWE) problem to groups). Our results on the cryptanalysis of this protocol tell us which instantiations of groups aren't suitable for this cryptosystem, thus leading to a better understanding for our search for suitable groups.

Affiliation

University of Cantabria, Spain

Author: ANUPINDI, Vishnupriya (University of Cantabria, Spain)

Co-author: E. AGATHOCLEOUS, A. BACHMAYR, C. MARTINDALE, R. Y. N. NCHIWO, M. STANOJKOVSKI

Presenter: ANUPINDI, Vishnupriya (University of Cantabria, Spain)

Session Classification: Applied Algebra and Number Theory