# Error correcting codes post quantum cryptography and IA

Valerie Gauthier Umaña

Universidad de los Andes

The arrival of quantum computers has posed a risk to the security of cryptography, particularly public key cryptography. To address this issue, a field known as post-quantum cryptography has been developed, which aims to enable secure communication on classical computers, assuming that the attacker has access to a quantum computer. One of the post-quantum families is based on error-correcting codes. Cryptosystems, like McEliece, rely on the fact correct errors, encoded by a random matrix is a NP-Complete problem. The main idea is to select a generator matrix of a code, that we know how to decode, such as a Goppa code, and disguise it as a random matrix. In 2019, Gohr proposed using machine learning methods to enhance existing attacks in symmetric cryptography. Our idea, inspired by Gohr's work, is to employ AI techniques to attempt error correction while assuming that the codes are disguised and, therefore, we do not know their structure. In this presentation, I will discuss some techniques we have explored.

In Special Session 40 on Network Coding and Related Fields at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS40-T05