WELINGTON SANTOS, University of Wisconsin Stout
Codes for Secure Distributed Matrix Multiplication

In this talk, we will explore how elements of coding theory can be applied to the problem of Secure Distributed Matrix Multiplication (SDMM). In this scenario, a user seeks to compute the product of two matrices, A and B, with the assistance of N honest-but-curious servers, ensuring that no server gains any information about either A or B. Specifically, we will introduce the HerA scheme, an SDMM model based on Hermitian codes. Additionally, we will demonstrate how matrix Reed-Solomon codes and their duality theory can be employed to detect malicious servers in the context of the SDMM problem.