

SPRING COLLOQUIUM SERIES

DR. HENRY CHIMAL- DZUL

UNIVERSITY OF TEXAS AT SAN ANTONIO

ERROR CORRECTING CODES AND POST-QUANTUM CRYPTOGRAPHY: AN INTRODUCTION AND TRENDS

Abstract: Error correcting codes are often implemented in modern applications (Wi-Fi, NASA Deep space communications, etc.) to correct errors introduced during storage and transmission of digital information. However, error correcting codes are also used in the latest developments of quantum science and technology. In this presentation, we discuss the basics of error correcting codes and their use in the design of cryptographic primitives that are conjectured to be resistant against attacks deployed using quantum technologies. While this talk will be introductory, we are also aiming to present some trends in the field of code-based cryptography.

FRIDAY MAY 2

3:00PM – 4:00PM

FLN 2.02.06

UTSA Mathematics