For favour of Posting

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

Department of Mathematics

SEMINAR ON PURE MATHEMATICS

The Discrete Fourier Transform of quadratic APN functions

by

Prof. Lukas Kölsch

University of South Florida

Abstract

(joint work with Sophie Hannah Bénéteau, Nicolas Goluboff, and Divyesh Vaghasiya)

Almost perfect nonlinear (APN) functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ play a central role as building blocks in the design of many block ciphers, serving as optimal functions to resist differential attacks. One of the most important properties of APN functions is their linearity, which is directly related to the Discrete Fourier Transform (DFT) of the function. In this talk, I shall establish two novel connections that allow us to derive strong conditions on the DFT of quadratic APN functions. We prove that the DFT of a quadratic APN function F operating on $n = 2k$ bits is uniquely associated with a vector space partition of $\mathbb{F}_2^n$ and a specific blocking set in the corresponding projective space $PG(n-1, 2)$. These connections give the first nontrivial results on the possible values of the DFT of quadratic APN functions.

Date : 18 December 2025 (Thursday)

Time : 10:00a.m.-11:00a.m.

Venue : Room 2129A (Lift 19)

All are Welcome!