



TED UNIVERSITY

Department of Mathematics

Seminars

Speaker	Dr. Oğuz Yayla
Email	oguz@metu.edu.tr
Affiliation	Department of Cryptology, IAM, METU
Date & Time	November 5, 2026 & 02:00pm
Room	K184

Algebraic Characterizations of MDS Matrices Against Structural Cryptanalysis

Abstract

Maximum Distance Separable (MDS) matrices over finite fields are fundamental building blocks in the design of diffusion layers for symmetric-key block ciphers, prized for achieving the theoretical maximum branch number. Yet, from the perspective of structural cryptanalysis, sharing an optimal branch number does not imply equivalent cryptographic strength. In particular, the existence of related differentials demonstrates that certain algebraic configurations within MDS matrices can be exploited in zero-difference attacks on AES-like architectures.

This seminar presents a comprehensive algebraic investigation into the related-differential resilience of MDS matrices over finite fields of characteristic two. We bridge coding-theoretic diffusion properties with differential cryptanalysis by establishing complete characterizations for small dimensions. Specifically, we show that while 2×2 MDS matrices never admit nontrivial related differentials, widely deployed structural families in dimension three namely, all 3×3 circulant and 3×3 involutory MDS matrices-always admit them. Furthermore, we present necessary and sufficient algebraic conditions that fully characterize related-differential resilience for arbitrary 3×3 and 4×4 MDS matrices. We conclude by discussing how these algebraic criteria reshape our understanding of linear diffusion layers in modern cipher design.

(Joint work with Ali Mert Sülge and Dr. Kamil Otal).