Indian Statistical Institute

Applied Statistics Unit

SEMINAR NOTICE

(Pre-Submission Seminar)

Speaker: Susanta Samanta

Title: Design and Analysis of MDS and Near-MDS Matrices and Their Application to Lightweight Cryptography

Date: 19 June, 2023

Time: 11:00AM

Venue:ASU Seminar Room

Online Platform: Google Meet (meet.google.com/nuf-upkp-edr)

Abstract: In this thesis, we focus on studying MDS and Near-MDS (NMDS) matrices and explore their construction in both recursive and nonrecursive settings. We present several theoretical results and analyze the hardware efficiency of MDS and NMDS matrix constructions.We begin by providing a comprehensive study of MDS matrices over finite fields. This study not only summarizes existing results but also reveals deep and nontrivial connections among various constructions of MDS matrices.

Next, we delve into the study of various sparse matrix structures for the construction of both MDS and NMDS matrices in recursive settings. Additionally, we explore various structures for the nonrecursive construction of NMDS matrices, including circulant and left-circulant matrices, as well as their generalizations such as Toeplitz and Hankel matrices. Whenever possible, we also make comparisons between the results of NMDS and MDS matrices.

Next, we present various techniques for direct constructions of MDS and NMDS matrices in both recursive and nonrecursive approaches. In the recursive approach, we derive recursive MDS and NMDS matrices from companion matrices, while direct constructions of nonrecursive MDS and NMDS matrices are obtained by using two generalized Vandermonde matrices. Furthermore, we propose a direct method for constructing involutory MDS and NMDS matrices.

Finally, we introduce FUTURE, a new SPN-based lightweight block cipher designed with minimal latency and low hardware implementation cost in mind. To achieve perfect diffusion, FUTURE incorporates an MDS matrix in its round function. While the use of MDS matrices in lightweight block ciphers is typically avoided due to their high implementation cost. The MDS matrix in FUTURE is composed of four sparse matrices, striking a balance between diffusion property and implementation cost. In addition, FUTURE adopts a lightweight yet cryptographically significant Sbox, which is formed by combining four different Sboxes. By combining these design choices, FUTURE successfully combines lightweight implementation with the desirable properties of MDS matrices, offering an effective solution for designing lightweight block ciphers.

All are invited to attend.