C R Rao Advanced Institute of Mathematics, Statistics & Computer Science (AIMSCS)

University of Hyderabad Campus, Prof. C R Rao Road, Gachibowli, Hyderabad, India 500 046

Website: http://crraoaimscs.org

Seminar

on

On the Diffusion Matrices for Lightweight block ciphers

by

Dr Sumanta Sarkar,

Scientist, TCS & Adjunct Faculty, CR Rao AIMSCS

Date and time :28 February 2017, Tuesday at 03:30 pm

Venue: Ramanujan Building, C R Rao AIMSCS

Abstract: Design of block ciphers is based on two fundamental principles - Confusion and Diffusion. Diffusion layer spreads the plaintexts statistics throughout the cipher texts. Maximum Distance Separable (MDS) matrices have the highest diffusion power. Therefore, the design of an efficient and lightweight MDS matrix directly impacts both the security and performance of a block cipher. In this talk I will speak on the constructions of efficient MDS matrices, where I will share some interesting new results.

Brief Biodata of Dr Sumanta Sarkar:

Sumanta Sarkar is a Scientist in TCS, Hyderabad and also an Adjunct Faculty of CR Rao AIMSCS. He did his masters in Mathematics at University of North Bengal and Ph D from Indian Statistical Institute, Kolkata under the supervision of Prof. Subhamoy Maitra. Sumanta has completed his Post Doctoral Research from INRIA Paris - Rocquencourt, France and University of Calgary.