Indian Statistical Institute, Chennai Centre

Seminar Announcement / संगोष्ठी की घोषणा

Date/ तारीख :6th June, 2017 (Tuesday).

Time/ समय : 3:30pm – 4:30pm.

Venue/ स्थान : SETS Auditorium, ISI-Chennai.

Speaker/वक्ता: Dr. Sumit Kumar Pandey, R. C. Bose Centre for Cryptology & Security, ISI, Kolkata.

Title/शीर्षक: Recursive MDS Diffusion Layers

Abstract: MDS matrices allow to build optimal diffusion layers in the design of block ciphers and hash functions. A recursive MDS matrix is an MDS matrix which can be expressed as a power of some companion matrix. The advantage of such a matrix is that it can be implemented by a single LFSR clocking several times. Such matrices are suitable for the design of diffusion layer in light-weight cryptographic applications. In this talk we will discuss some constructions of recursive MDS matrices.

सभी को आमंत्रित कर रहे हैं| All are invited.