ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dipartimento di Matematica e Fisica
Segreteria per la Ricerca

SEMINARIO di CRITTOGRAFIA

Prof. Roberto LA SCALA

(Dipartimento di Matematica, Università di Bari)

CIFRARI A FLUSSO DEFINITI DA SISTEMI DI EQUAZIONI ALLE DIFFERENZE SU CAMPI FINITI E LORO CRITTANALISI

Lunedì 30 Settembre 2024

ore 14h00

Via della Vasca Navale 84

AULA B

Abstract: Diversi cifrari a flusso di interesse applicativo, come Trivium ed E0 del Bluetooth, possono essere modellizzati come sistemi di equazioni (ordinarie esplicite) alle differenze a coefficienti e soluzioni su campi finiti. Tali equazioni governano infatti l'evoluzione lungo un tempo discreto del registro di questi cifrari che è un vettore ad entrate in un campo finito. I valori ai diversi istanti di tempo di una funzione polinomiale del registro determinano quindi il keystream. L'uso della teoria formale delle equazioni alle differenze consente lo studio di alcune proprietà fondamentali di tali cifrari a flusso, quali la loro invertibilità e periodicità. Su questo studio si basa anche una definizione precisa di alcuni attacchi algebrici utili a valutare la sicurezza di questi "cifrari alle differenze". Tale modellizzazione e la corrispondente crittoanalisi consentono quindi lo sviluppo di nuovi sistemi crittografici sicuri.

per informazioni: Prof. Marco Pedicini