Miniworkshop
Coding Theory and Cryptography

Dipartimento di Matematica
Università degli Studi di Torino
Via Carlo Alberto 8/10, Torino
13-14 Ottobre 2014

Programma

Lunedì 13 ottobre 2014

9.00 - 9.30 **Apertura dei lavori**
9.30 - 11.30 **Funzioni booleane e la loro applicazione alla crittografia e ai codici**
Prof. Massimiliano Sala (Università degli Studi di Trento)
11.30 - 12.00 **Coffee break**
12.00 - 13.00 **Codici Hermitiani e parole di peso piccolo**
Dott. ssa Chiara Marcolla (Università degli Studi di Trento)

13.00 - 14.30 **Pausa Pranzo**

14.30 - 15.30 **Introduzione ai codici a fontana**
Dott. Valerio Bioglio (Politecnico di Torino)
15.30 - 16.30 **Polinomi locatori sparsi per codici ciclici binari**
Dott. ssa Michela Ceria (Università degli Studi di Torino)
16.30 - 17.00 **Coffee break**
17.00 - 18.00 **Index coding**
Dott. Marco Calderini (Università degli Studi di Trento)

Martedì 14 ottobre 2014

9.30 - 11.30 **Una introduzione alla crittografia: RSA, gli attacchi di Shamir, le Curve Ellittiche**
Prof. Teo Mora (Università degli Studi di Genova)
11.30 - 12.00 **Coffee break**
12.00 - 13.00 **Calcolo di multipli di peso basso di polinomi binari attraverso il logaritmo discreto**
Dott. ssa Claudia Tinnirello (Università degli Studi di Trento)

13.00 - 14.30 **Pausa Pranzo**

14.30 - 15.30 **Successioni di punti su coniche mediante funzioni di Rédei generalizzate**
Dott. Nadir Murru (Università degli Studi di Torino)
15.30 - 16.30 **Curve ellittiche nella rappresentazione di interi tramite forme quadratiche binarie**
Dott. Federico Pintore (Università degli Studi di Trento)
16.30 - 17.00 **Coffee break**
17.00 - 18.00 **Tavola Rotonda**