Unità di Ricerca dell'Istituto Nazionale di Alta Matematica
presso l'Università dell'Aquila

1st workshop in Algebra for Cryptography

A4C2019

Thursday 10th October

14:30 – 15:10
Francesca Dalla Volta (Università Milano-Bicocca)
Computation of the Moebius function for PSL(3, 2^p) and some related topics
15:10 – 16 40
Alessio Meneghetti (Università di Trento)
A formula on the weight distribution of codes
16:40 – 17:00
Coffee Break
17:00 – 17:45
Federico Pintore (University of Oxford)
An isogeny-based signature with tight security
17:45 – 18:25
Marco Calderini (University of Bergen)
On vectorial Boolean functions with low differential and boomerang uniformity

Friday 11th October

10:30 – 11:00
Maria Tota (Università di Salerno)
On the primitivity of PRESENT and other lightweight ciphers (Abstract)
11:00 – 11:40
Nadir Murru (Università di Torino)
The Pell conic in cryptography
11:40 – 12:00
Coffee Break
12:00 – 12:40
Roberto Civino (Università dell'Aquila)
Regular subgroups with large intersection
12:40 – 13:10
Ilaria Colazzo (Vrije Universiteit Brussel)
Braces: between regular subgroups and solutions of the Yang-Baxter equation

INδAM

disim

University of L'Aquila - DISIM

Aula Alan Turing - Blocco 0

ORGANIZED BY
Riccardo Aragona * Roberto Civino
Noberto Gavioli * Carlo Maria Scoppola