Dipartimento di Matematica e Fisica
18-22 July 2022

CONTEMPORARY ALGEBRAIC AND GEOMETRIC TECHNIQUES IN CODING THEORY AND CRYPTOGRAPHY

(Virtual Summer School on Microsoft TEAMS)

The School aims at bringing together Master/PhD students, academics and security experts from industry in order to see how sophisticated algebraic and geometric methods have been applied in recent years to construct error-correcting codes and to define secure cryptosystems.

The School includes a program of multi-disciplinary studies within one week and offers 4 courses in which geometric and algebraic tools will be developed in order to investigate coding theory and cryptography. In addition, there will be a programming session devoted to the modelling and analysis of security protocols with the Tamarin Prover, a session in which industries will enlighten how codes and cryptographic systems play a crucial role in modern technologies and a contributed talk session for young researchers with high profile, where the best presentation will be awarded. Also, there will be a lecture "De Componendis Cifris: a national initiative" by Prof. Massimiliano Sala from University of Trento.

www.matfis.unicampania.it/summer-school
codecryptoschool22@unicampania.it

Lectures

- Introduction to FHE and the TFHE scheme
(Dr. Ilaria Chillotti Zama - France)
- Post-quantum group-based cryptography
(Prof. Delaram Kahrobaei, City University of New York - USA)
- Network coding
(Prof. Alberto Ravagnani, Eindhoven University of Technology - the Netherlands)
- Linear Codes and Galois Geometries
(Prof. Leo Storme, Ghent University - Belgium)

Programming session

Experiencing formal modelling and analysis of protocol security with the Tamarin Prover
(Dr. Mariapia Raimondo, Università degli Studi della Campania "Luigi Vanvitelli")

Industrial session

Secure element technology and Cryptography
(STMicroelectronics)
Digital Stamp
(Ing. Nicola Fedele - CEO Bluenet Technologies)

Timeline

- Abstract submission deadline:
30 April 2022
- Acceptance notification:
31 May 2022
- Registration deadline:
31 May 2022

Chair:

Ferdinando Zullo

Scientific committee:

Stefano Marrone
Olga Polverino
Antonio Tortora

Organizers:

Vito Napolitano
Roberta De Fazio
Maria Ferrara
Paolo Santonastaso

Università
degli Studi
della Campania
Luigi Vanvitelli

Dipartimento di
Matematica e Fisica

www.decifris.it

www.matfis.unicampania.it
www.unicampania.it