Cryptography and Coding Theory

The conference, in memory of Emeritus Professor Michele Elia, is organized by the " Crittografia e Codici" group of the UMI (Italian Mathematical Union) and the national cryptography initiative De Componendis Cifris.

The event will take place **virtually** on **September 21-22, 2021** at the University of L'Aquila.

Cryptography and coding theory are fields of study and research, which find wide application in data and transmission protection, as well as in cyber security.

The conference will feature **researchers, companies and high school teachers**, each presenting their own approach to this fascinating topic.

The initiatives of the **national cryptographic community** will also be presented and awards will be given to the winning students of the National Cryptographic Challenge.

Conference outline

21th September 2021		*22th September 2022*	
9:00 - 9:30	**Opening and greetings**	9:00 - 9:50	**Institutional greetings ***
9:30 -11:20	**First scientific session**	9:50 - 11:30	Community session *
11:50 - 13:40	**Second scientific session**	11:40 - 13:30	**Fourth scientific session**
14:45 - 16:45	Educational and outreach session *	14:45 - 16:45	Corporate research session
17:00 - 19:10	**Third scientific session**	17:00 - 18:50	**Fifth scientific session**

** Session to be held in Italian

21 September 2021

OPENING AND GREETINGS

09:00 **Guido Proietti** - Head of the Department DISIM - Università degli Studi dell'Aquila
09:10 **Massimiliano Sala** - Acting Director of De Componendis Cifris
09:20 **Norberto Gavioli** - Coordinator of the group Crittografia e Codici - Unione Matematica Italiana

FIRST SCIENTIFIC SESSION

09:30 **Joachim Rosenthal** - ***The work of Michele Elia on continued fractions and factoring***
10:20 **Elena Berardini** - ***Riemann–Roch spaces and algebraic geometry codes***
10:40 **Martino Borello** - ***On short minimal codes and related combinatorial structures***
11:00 **Gianira Alfarano** - ***Roos-like bound for skew-cyclic codes in Hamming and (sum-)rank metric***

SECOND SCIENTIFIC SESSION

11:50 **Alessio Caminata** - ***Degrees of regularity***
12:40 **Christopher Battarbee** - ***Cryptanalysis of semidirect product key exchange***
13:00 **Leyla Işık** - ***On the index of the Diffie-Hellman mapping***
13:20 **Marco Calderini** - ***On the existence of certain APN functions over F_2^(3m)***

EDUCATIONAL AND OUTREACH SESSION*

14:45 **Saluti. Francesca Tovena -Claudio Bernardi** - Gruppo UMI Licei Matematici
15:05 **Michael Lodi** - ***Crittografia a blocchi al Liceo Matematico***
15:25 **Carola Manolino and Matteo Torre** - Intervento di storia della crittografia
L'arte di nascondere i messaggi: dalla scitala alle macchine cifranti, passando per il disco di Alberti
15:45 **Paola Morando and Silvia Pagani** - ***Errori di trasmissione: un bit per trovarli, tre bit per incatenarli***
16:05 **Alexander Saltuari** - ***Opportunità didattiche offerte dalla Crittografia al Liceo Matematico***
16:25 **Manuela Saponaro** - ***Tra passato e futuro : la crittografia nella scuola secondaria di primo grado***

THIRD SCIENTIFIC SESSION

17:00 **Relinde Jurrius** - ***q-Analogues in codes and related combinatorics***
17:50 **Edoardo Persichetti** - ***LESS-FM: Fine-tuning signatures from the code equivalence problem***
18:10 **Federico Pintore** - ***Explicit formulas for hashing into G_2 on BLS pairing-friendly curves***
18:30 **Paolo Santonastaso** - ***On the list decodability of rank-metric codes***
18:50 **Heide Gluesing-Luerssen** - ***Independent spaces of q-polymatroids***

22 September 2021 (morning)

SALUTI ISTITUZIONALI*

9:00 Generale di Corpo d'Armata **Luigi Francesco De Leverano**
Consigliere Militare del Presidente del Consiglio dei Ministri

9:10 Dott. **Ivano Gabrielli**
Primo Dirigente della Polizia di Stato -Servizio Polizia Postale e delle Comunicazioni
III Divisione - CNAIPIC - Direttore

9:20 Colonnello **Antonio Buccoliero**
Vice Comandante della Legione Carabinieri Abruzzo e Molise

9:30 Colonnello **Gianluca Berruti**
Vice Comandante del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche G.d.F.

9:40 Onorevole Deputato **Davide Zanichelli**
Coordinatore intergruppo parlamentare criptovalute e blockchain

COMMUNITY SESSION*

9:50 **Massimiliano Sala** - **Le attività dell'iniziativa nazionale di crittografia De Componendis Cifris**
10:10 **Premiazione vincitori delle CryptoWars 2020 e presentazione delle CryptoWars 2021**
10:15 **Ivan Visconti** - **Le attività del team CifrisChain sulla tecnologia Blockchain e le Crittovalute**
10:30 **Marco Pedicini** - **Le attività del team CifrisCloud sulla Cloud Encryption e le sue applicazioni**
10:45 **Marco Baldi** - **Le attività del team PQCifris sulla Crittografia Post-Quantum**
11:00 **Massimo Giulietti** - **L'advisory Board De Cifris: un ponte tra accademia e aziende**
11:15 **Massimiliano Sala** - **Un ricordo del nostro Presidente Michele Elia**

FOURTH SCIENTIFIC SESSION

11:40 **Sihem Mesnager** -
Reader's digest of 17-year achievements on Boolean and vectorial functions and open problems

Parallel sessions	I	II	III
12:30	**M. Á. Navarro Pèrez** *Optimum distance flag codes and Singer groups*	**Francesco Pavese** *Small complete caps in PG(4n + 1, q)*	**Amir Hamzah Abd Ghafar** *Partial key exposure attack on RSA using Dickman's function*
12:50	**Marco Timpanella** *PIR codes from combinatorial structures*	**Wissam Ghantous** *Loops, multi-edges and collisions in isogeny graphs*	**Giuseppe Cotardo** *Codes for the binary asymmetric channel*
13:10	**Stefano Lia** *AG codes from F_q 7-rational points of the GK maximal curve*	**Annamaria Iezzi** *Bruhat–Tits trees as a cryptanalytic tool for isogeny-based cryptography*	**Alessandro Budroni** *A new trapdoor construction for LWE (Learning With Error)*

22 September 2021 (afternoon)

CORPORATE RESEARCH SESSION

14:45 **Matteo Bocchi and Adriano Gaibotti -** ***Hash-based post-quantum signatures on 32-bit microcontrollers***

15:05 **Niccolò Izzo** - ***Compute express link security***

15:25 **Davide Bacco** - ***Quantum key distribution for telecom applications***

15:45 **Paolo Gasti** - ***Keyless: a privacy-preserving biometric authentication system***

16:05 **Andrea Molino** - ***Cryptography for electronic locks in security doors***

FIFTH SCIENTIFIC SESSION

17:00 **Elisa Gorla** - ***A general theory of supports and generalized weights for linear codes***

Parallel sessions	I	II	III
17:50	**Giovanni Longobardi** *Partially scattered linearized polynomials, linear sets and rank metric codes*	**Ilaria Zappatore** *A fault-tolerant technique for polynomial linear system Solving*	**Jonathan Mannaert** *On the non-existence of Cameron-Liebler sets of k-spaces in PG(n, q)*
18:10	**Giovanni Zini** *On a class of linear square MRD codes*	**Enrico Piccione** *An algebraic attack on the WG-PRNG stream cipher*	**Emanuele Giunta** *On interactive oracle proofs for boolean R1CS statements*
18:30	**Wrya K. Kadir** *On interpolation-based decoding of MRD codes*	**Isaac Canales Martínez** *Multivariate correlation attacks and the cryptanalysis of LFSR-based stream ciphers*	

SPEAKERS

INVITED

Alessio Caminata (University of Genova)
Elisa Gorla (University of Neuchâtel)
Relinde Jurrius (Netherlands Defence Academy)
Sihem Mesnager (University of Paris VIII)
Joachim Rosenthal (University of Zurich)

EDUCATIONAL AND OUTREACH SESSIONS

Michael Lodi (Università di Bologna)
Carola Manolino (Università di Torino)
Paola Morando (Università di Milano)
Silvia Pagani (Università Cattolica del Sacro Cuore)
Alexander Saltuari (Liceo "Majorana" Roma)
Manuela Saponaro (Istituto "Commenda" Brindisi)
Matteo Torre (Liceo "G. Peano" di Tortona)

- COMMUNITY SESSION

Marco Baldi (Università Politecnica delle Marche)
Massimo Giulietti (Università degli Studi di Perugia)
Marco Pedicini (Università degli studi Roma Tre)
Massimiliano Sala (Università degli Studi di Trento)
Ivan Visconti (Università degli Studi di Salerno)

CORPORATE RESEARCH SESSION

Davide Bacco (Technical University of Denmark)
Matteo Bocchi (STMicroelectronics)
Adriano Gaibotti (STMicroelectronics)
Paolo Gasti (Keyless)
Niccolò Izzo (Micron Technology Inc.)
Andrea Molino (Dierre S.P.A.) *s*

SCIENTIFIC SESSIONS

Gianira Alfarano (University of Zurich)
Amir H: Abd Ghafar (Universiti Putra Malaysia)
Christopher Battarbee (University of York)
Elena Berardini (École Polytechnique - LIX)
Martino Borello (Université Paris 8 - LAGA
Alessandro Budroni (University of Bergen)
Marco Calderini (University of Bergen)
Isaac Canales Martínez (University of Bergen)
Giuseppe Cotardo (University College Dublin)
Wissam Ghantous (University of Oxford)
Emanuele Giunta (IMDEA - Scuola Sup. di Catania)
Heide Gluesing-Luerssen (University of Kentucky)

Annamaria Iezzi (Université de la Pol. Française)
Wrya K. Kadir (University of Bergen)
Leyla Işık (İstinye University)
Stefano Lia (University of Basilicata)
Giovanni Longobardi (University of Padua)
Jonathan Mannaert (Vrije Universiteit Brussel)
Miguel Ángel Navarro Pérez (University of Alicante)
Francesco Pavese (Polytechnic University of Bari)
Edoardo Persichetti (Florida Atlantic University) -
Enrico Piccione (University of Trento)
Federico Pintore (University of Bari)
Paolo Santonastaso (Universiy of Campania)
Marco Timpanella (University of Campania
Ilaria Zappatore (LIX - Inria Saclay)
Giovanni Zini (University of Campania)

Organizing Committee

Chairs: *Norberto Gavioli (University of L'Aquila) -- Massimiliano Sala (University of Trento)*

Members: *Riccardo Aragona (University of L'Aquila), Danilo Bazzanella (Polytechnic University of Turin), Guido Bertoni (Security Pattern), Vittoria Bonanzinga (University of Reggio Calabria), Matteo Bonini (University College Dublin), Michela Ceria (Polytechnic University of Bari), Giulio Codogni (Tor Vergata University of Rome), Luca De Feo (IBM Zurich), Eleonora Guerrini (University of Montpellier), Roberto La Scala (University of Bari), Alessia Marelli (B&A consulting), Alessio Meneghetti (University of Trento), Teo Mora (University of Genova), Guglielmo Morgari (Telsy), Nadir Murru (University of Trento), Emmanuela Orsini (COSIC, KU Leuven), Elisabetta Pastori (St. Stephen's School of Rome), Giordano Santilli (University of Trento), Cristian Tirelli (University of Italian Switzerland), Maria Tota (University of Salerno), Vincenzo Vespri (University of Florence), Ferdinando Zullo (University of Campania)*

Web pages:

- https://sites.google.com/view/crittografiaecodici/convegno-annuale

www.decifris.it -- umi.dm.unibo.it

Contacts:

matematica@decifris.it

Cryptography and Coding Theory