

## CACT & CAAFRA

Wed 2014-07-09

- **11am - 11:30am**  
**An overview on algebraic invariants and the main parameters of some parametrized codes**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** M.G. Sarabia, C. Rentería Márquez, E. Sarmiento Rosales
- **11:30am - 12pm** **Evaluation Codes and Weierstrass Semigroups**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Emma Previato
- **12pm - 12:30pm** **Error correcting pair: a new approach to Code-based Cryptography**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** I. Marquez-Corbella, Ruud Pellikaan
- **2pm - 2:30pm** **On the Efficiency of Shortened Cyclic Multiple-Burst-Correcting Codes**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Ana Lucila Sandoval Orozco, Luis Javier García Villalba, Mario Blaum
- **2:30pm - 3pm** **Edge-weighted Cayley graphs and p-ary bent functions**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** David Joyner
- **3pm - 4pm** **BoF Meeting on SAGE and Coding Theory**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro

Thu 2014-07-10

- **8:30am - 9am** **Exponents of Skew Polynomials**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Ahmed Cherchem, André Leroy
- **9am - 9:30am** **The Module Isomorphism Problem for Finite Rings and Related Results**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Iuliana Ciocanea Teodorescu
- **9:30am - 10am** **Construction of codes for DNA computing by the Greedy Algorithm**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Nabil Bennenni, Kenza Guenda, T. Aaron Gulliver
- **10am - 10:30am** **Multivariable Codes in Principal Ideal Polynomial Quotient Rings**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Edgar Martinez-Moro
- **2pm - 2:30pm** **A Johnson-Type Bound for Group Codes and Lattices**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Malihe Aliasgari, Mohammad-Reza Sadeghi

## CACT & CAAFRA

- 2:30pm - 3pm The degree compatible Gröbner Fan for Linear Codes**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Natalia Dück, I. Márquez-Corbella, Edgar Martínez-Moro
- 3pm - 3:30pm Binomial Ideal Associated to a Lattice and Its Label Code**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Malihe Aliasgari, Daniel Panario, Mohammad-Reza Sadeghi
- 3:30pm - 4pm The extended and generalized rank weight enumerator of a code**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Relinde Jurrius, Ruud Pellikaan

Fri 2014-07-11

- 8:30am - 9am Extending Construction X for Quantum Error-Correcting Codes**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Akshay Degwekar, Kenza Guenda, T. Aaron Gulliver
- 9am - 9:30am A notion of multivariate BCH bounds and codes**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** José Joaquín Bernal Buitrago, Diana Haidive Bueno Carreño, Juan Jacobo Simón Pinero
- 9:30am - 10am**  
**HIMMO: A collusion-resistant identity-based scheme for symmetric key generation**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Oscar García-Morchón, Ronald Rietman, Ludo Tolhuizen, Domingo Gómez, Jaime Gutiérrez
- 10am - 10:30am**  
**McEliece Cryptosystem Based on Punctured Convolutional Codes and the Pseudo-Random Generators**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Hamza Moufek, Kenza Guenda
- 11am - 11:30am**  
**: A New Non-Associative Cryptosystem Based on NTOW Public Key Cryptosystem and Octonions Algebra**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Kadijeh Bagheri, Mohammad-Reza Sadeghi
- 11:30am - 12pm Network Coding via Skew Polynomials**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Felice Man-ganiello
- 12pm - 12:30pm Computer Algebra Challenges for Constructing Skew Cyclic Codes**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Noah Aydin
- 2pm - 2:30pm Some applications of idempotent semirings in Public Key Cryptography**  
**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Mariana Durcheva

## CACT & CAAFRA

### 2:30pm - 3pm Plaintext Recovery for One-Time Pads Used Twice

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Gregory V. Bard, Theodore McDonough

### 3pm - 3:30pm Some new almost difference sets via finite fields

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Bo Phillips, Jace Robinson

### 3:30pm - 4pm Some results on finite fields

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** James Hufford

### 4pm - 5pm BoF Meeting on SAGE

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** <http://www.singacom.uva.es/~edgar/BoFSAGE/>

Sat 2014-07-12

### 8:30am - 9am T.B.A.

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Steve Szabo

### 9am - 9:30am Codes Over Rings of Order 16

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Steven Dougherty, Esengül Saltürk, Steve Szabo

### 9:30am - 10am Codes over local rings of order 16 and their Gray maps

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Steven Dougherty, Esengül Saltürk

### 10am - 10:30am

#### On Gröbner Bases over Rings and Residue Class Polynomials Rings with Torsion

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Ambedkar Dukkipati, Nithish Pai, Maria Francis, Abhishek Dubey

### 11am - 11:30am On a class of difference set pairs

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** Ankita Bakshi, Deeksha

### 11:30am - 12pm Difference Set Pairs : A Recursive Approach via group rings

**Calendar:** CACT2014  
**Created by:** Edgar Martinez-Moro  
**Description:** K.T.Arasu, Anika Goyal , Abhishek Puri