

## CACT & CAAFRA

Wed 2014-07-09

- **11am - 11:30am**  
**An overview on algebraic invariants and the main parameters of some parametrized codes**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** M.G. Sarabia, C. Rentería Márquez, E. Sarmiento Rosales
  
- **11:30am - 12pm** **The extended and generalized rank weight enumerator of a code**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Relinde Jurrius, Ruud Pellikaan
  
- **12pm - 12:30pm** **Error correcting pair: a new approach to Code-based Cryptography**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** I. Marquez-Corbella, Ruud Pellikaan
  
- **2pm - 2:30pm** **On the Efficiency of Shortened Cyclic Multiple-Burst-Correcting Codes**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Ana Lucila Sandoval Orozco, Luis Javier García Villalba, Mario Blaum
  
- **2:30pm - 3pm** **Edge-weighted Cayley graphs and p-ary bent functions**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** David Joyner
  
- **3pm - 4pm** **BoF Meeting on SAGE and Coding Theory**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com

Thu 2014-07-10

- **8:30am - 9am** **The degree compatible Gröbner Fan for Linear Codes**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Natalia Dück, I. Márquez-Corbella, Edgar Martínez-Moro
  
- **9am - 9:30am** **Binomial Ideal Associated to a Lattice and Its Label Code**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Malihe Aliasgari, Daniel Panario, Mohammad-Reza Sadeghi
  
- **9:30am - 9:45am** **A Johnson-Type Bound for Group Codes and Lattices**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Malihe Aliasgari, Mohammad-Reza Sadeghi
  
- **10am - 10:15am** **Evaluation Codes and Weierstrass Semigroups**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Emma Previato
  
- **2pm - 2:30pm** **Exponents of Skew Polynomials**  
**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Ahmed Cherchem, André Leroy

## CACT & CAAFRA

### 2:30pm - 3pm The Module Isomorphism Problem for Finite Rings and Related Results

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Iuliana Ciocanea Teodorescu

### 3pm - 3:30pm Construction of codes for DNA computing by the Greedy Algorithm

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Nabil Bennenni, Kenza Guenda, T. Aaron Gulliver

### 3:30pm - 4pm Multivariable Codes in Principal Ideal Polynomial Quotient Rings

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Edgar Martinez-Moro

Fri 2014-07-11

### 8:30am - 9am

**HIMMO: A collusion-resistant identity-based scheme for symmetric key generation**

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Oscar García-Morchón, Ronald Rietman, Ludo Tolhuizen, Domingo Gómez, Jaime Gutiérrez

### 9am - 9:30am On a class of difference set pairs

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Ankita Bakshi, Deeksha

### 9:30am - 10am Stickelbergers Congruences and Perfect Sequence constructions

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** K.T.Arasu, Anika Goyal, Abhishek Puri

### 10am - 10:30am

**McEliece Cryptosystem Based on Punctured Convolutional Codes and the Pseudo-Random Generators**

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Hamza Moufek, Kenza Guenda

### 11am - 11:30am

**A New Non-Associative Cryptosystem Based on NTOW Public Key Cryptosystem and Octonions Algebra**

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Kadijeh Bagheri, Mohammad-Reza Sadeghi

### 11:30am - 12pm Network Coding via Skew Polynomials

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Felice Man-ganiello

### 12pm - 12:30pm Computer Algebra Challenges for Constructing Skew Cyclic Codes

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Noah Aydin

### 2pm - 2:30pm Some applications of idempotent semirings in Public Key Cryptography

**Calendar:** CACT & CAAFRA

**Created by:** edgar.martinezmoro@gmail.com

**Description:** Mariana Durcheva

## CACT & CAAFRA

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

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Gregory V. Bard, Theodore McDonough

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

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Bo Phillips, Jace Robinson

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

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** James Hufford

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

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** <http://www.singacom.uva.es/~edgar/BoFSAGE/>

Sat 2014-07-12

### 8:30am - 9am

**Linear Codes over  $Z_4[x]/(x^2-2x)$ . Dual Preserving Maps and Images as Codes over  $Z_4$**

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Steve Szabo

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

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Steven Dougherty, Esengül Saltürk, Steve Szabo

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

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Steven Dougherty, Esengül Saltürk

### 10am - 10:30am

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

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Ambedkar Dukkipati, Nithish Pai, Maria Francis, Abhishek Dubey

### 11am - 11:30am A notion of multivariate BCH bounds and codes

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** José Joaquín Bernal Buitrago, Diana Haidive Bueno Carreño, Juan Jacobo Simón Pinero

### 11:30am - 12pm Extending Construction X for Quantum Error-Correcting Codes

**Calendar:** CACT & CAAFRA  
**Created by:** edgar.martinezmoro@gmail.com  
**Description:** Akshay Degwekar, Kenza Guenda, T. Aaron Gulliver