

School of Computer Science  
Complutense University of Madrid, Spain

---

Workshop Program

# International Workshop on the Arithmetic of Finite Fields

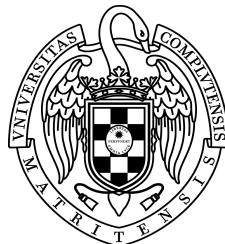
## WAIFI 2007

June 21-22, 2007, Madrid, Spain

---

### Sponsors

Group of Architecture and Technology of Computer Systems  
School of Computer Science, Complutense University  
Spanish Ministry of Education and Science  
Spanish Mathematical Royal Society  
Complutense University, Madrid, Spain  
Dirección General de Universidades e Investigación, Consejería de  
Educación, Comunidad de Madrid



Thursday 21st June, 2007

09:00 - 09:30 Registration

09:30 - 09:40 Welcome

9:40 - 10:40 Invited Talk by Harald Niederreiter

*Factorization of polynomials over finite fields using differential equations*

**Session 1: Structures in Finite Fields**

10:40 - 11:05 *Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields* by Robert W. Fitzgerald and Joseph L. Yucas

11:05 - 11:30 *A note on modular forms on finite upper half planes* by Yoshinori Hamahata

11:30 - 11:55 Coffee Break

**Session 2: Efficient Implementation and Architectures**

11:55 - 12:20 *A Coprocessor for the Final Exponentiation of the  $\eta_T$  Pairing in Characteristic Three* by Jean-Luc Beuchat, Nicolas Brisebarre, Masaaki Shirase, Tsuyoshi Takagi and Eiji Okamoto

12:20 - 12:45 *VLSI Implementation of a Functional Unit to Accelerate ECC and AES on 32-bit Processors* by Stefan Tillich and Johann Großschädl

12:45 - 13:10 *Efficient multiplication using type 2 optimal normal bases* by Joachim von zur Gathen, Amin Shokrollahi and Jamshid Shokrollahi

13:10 - 14:45 Lunch Break

**Session 3: Efficient Finite Field Arithmetic**

14:45 - 15:10 *Effects of Optimizations for Software Implementations of Small Binary Field Arithmetic* by Roberto Avanzi and Nicolas Thériault

15:10 - 15:35 *Software implementation of arithmetic in  $GF(3^m)$*  by Omran Ahmadi, Darrel Hankerson and Alfred Menezes

15:35 - 16:00 *Complexity Reduction of Constant Matrix Computations over the Binary Field* by Oscar Gustafsson and Mikael Olofsson

16:00 - 16:25 *Towards Optimal Toom-Cook Multiplication for Univariate and Multivariate Polynomials in Characteristic 2 and 0* by Marco Bodrato

16:25 - 16:55 Coffee Break

**Session 4: Classification and Construction of Mappings over Finite Fields**

16:55 - 17:20 *A construction of differentially 4-uniform functions from commutative semifields of characteristic 2* by Nobuo Nakagawa and Satoshi Yoshiara

17:20 - 17:45 *Complete Mapping Polynomials over Finite Field  $F_{16}$*  by Yuan Yuan, Yan Tong and Huanguo Zhang

17:45 - 18:10 *On the Classification of 4 Bit S-boxes* by G. Leander and A. Poschmann

18:10 - 18:35 *The simplest method for constructing APN polynomials EA-inequivalent to power functions* by Lilya Budaghyan

20:45 - Gala Dinner at Meliá Madrid Princesa hotel

Rooms: Salas Cibeles I and Cibeles II

Friday 22th June, 2007

**9:00 - 10:00 Invited Talk by Richard E. Blahut**

*An Engineer Looks at the Turyn Representation*

**Session 5: Curve Algebra**

**10:00 - 10:25** *New Point Addition Formulae for ECC Applications* by Nicolas Meloni

**10:25 - 10:50** *Explicit formulas for real hyperelliptic curves of genus 2 in affine representation* by Stefan Erickson, Michael J. Jacobson, Jr., Ning Shang, Shuo Shen and Andreas Stein

**10:50 - 11:15** *The Quadratic Extension Extractor for (Hyper)elliptic Curves in Odd Characteristic* by Reza Rezaeian Farashahi and Ruud Pellikaan

**11:15 - 11:45 Coffee Break**

**Session 6: Cryptography**

**11:45 - 12:10** *On Kabatianskii-Krouk-Smeets Signatures* by Pierre-Louis Cayrel, Ayoub Otmani and Damien Vergnaud

**12:10 - 12:35** *Self-certified signatures based on discrete logarithms* by Zuhua Shao

**12:35 - 13:00** *Attacking the Filter Generator over  $GF(2^m)$*  by Sondre Rønjom and Tor Helleseth

**13:00 - 14:35 Lunch Break**

**Session 7: Codes**

**14:35 - 15:00** *Cyclic additive and quantum stabilizer codes* by Jürgen Bierbrauer

**15:00 - 15:25** *Determining the Number of One-weight Cyclic Codes when Length and Dimension are Given* by Gerardo Vega

**15:25 - 15:50** *Error correcting codes from quasi-Hadamard matrices* by V. Álvarez, J.A. Armario, M.D. Frau, E. Martin and A. Osuna

**15:50 - 16:15** *Fast Computations of Gröbner Bases and Blind Recognitions of Convolutional Codes* by Peizhong Lu and Yan Zou

**16:15 - 16:45 Coffee Break**

**Session 8: Discrete Structures**

**16:45 - 17:10** *A twin for Euler's  $\phi$  function in  $\mathbf{F}_2[X]$*  by R. Durán Díaz, J. Muñoz Masqué and A. Peinado Domínguez

**17:10 - 17:35** *Discrete phase-space structures and mutually unbiased bases* by A. B. Klimov, J. L. Romero, G. Björk and L. L. Sánchez-Soto

**17:35 - 18:00** *Some Novel Results of  $p$ -adic Component of Primitive Sequences over  $Z/(p^d)$*  by Yuewen Tang and Dongyang Long