CAI 2017 Program

June 25-28, 2017

http://www.cargo.wlu.ca/CAI2017/

Sunday, June 25, 2017
10 a.m. – 16 p.m. Conference Registration, Hotel Elite Conference Center, 2nd floor
17:00 p.m. – 18:00 p.m. **Track 5: Natural and Quantum Computing** **Track 5 Chair: Mika Hirvensalo (Finland)** **Track 5: Invited Speaker** **Lila Kari (University of Waterloo, Canada)** **Was Pegasus a mammal or a bird? How to measure and visualize (real or synthetic) species' relatedness**
18:00 p.m. – 18:30 p.m. **Interference as a computational resource** **Mika Hirvensalo**
18:30 p.m. – 19:00 p.m. **Branching Program Complexity of Quantum Hashing** **Farid Ablayev, Marat Ablayev**
19:00 p.m. – 19:30 p.m. **Resistance Analysis for Quantum Hashing** **Farid Ablayev, Marat Latypov, Alexander Vasiliev, Artur Vasilov**

Kosmos Rent-a-Car Reservation Team

Address: 5 Syngrou Ave. 11743

Athens, Greece

Phone: +30 210 9234695-8,

Fax: +30 210 9243564

Email: info@kosmos-carrental.com

http://www.kosmos-carrental.com/

10% off the quoted Internet price, to CAI 2017 participants

Monday, June 26, 2017
9:00 a.m. – 10:00 a.m. **Track 3: Computer Algebra** **Track 3 Chairs: Rafael Sendra (Spain), Franz Winkler (Austria)** **Track 3: Invited Speaker** **Michael Wibmer (University of Pennsylvania, USA)** **Computing difference algebraic relations among solutions of linear differential equations**
10:00 a.m. – 10:30 a.m. **Ioannis Z. Emiris, Konstantinos Gavriil, Christos Konaxis** **Interpolation of syzygies for implicit matrix representation**
10:30 a.m. – 11:00 a.m. **Christoph Fürst, Günter Landsmann** **Reduction in free modules**
11:00 a.m. – 11:30 a.m COFFEE BREAK
11:30 a.m. – 12:00 a.m. **Philippe T. Gimenez** **Constructing small cellular free resolutions for monomial ideals**
12:00 a.m. – 12:30 p.m. **Takis (Panajiotis) Sakkalis** **Quaternion polynomials: Roots and their Jacobians**
12:30 p.m. - 13:00 p.m. **J. Horacek, Martin Kreuzer, A.S. Messeng Ekossono** **A signature based border basis algorithm**
13:00 p.m. – 13:30 p.m. **Günter Landsmann, Christoph Fürst** **Gröbner reduction in modules over arbitrary rings**
13:30 p.m. – 15:00 p.m LUNCH BREAK
15:00 p.m. – 15:30 p.m. **Specialization of Symbolic Polynomials, Stephen Watt**
15:30 p.m. – 16:00 p.m. **G.H.E. Duchamp, Hoang Ngoc Minh, Quoc Hoan Ngo** **The algebra of Kleene stars of the plane and polylogarithms**
16:00 p.m. – 16:30 p.m. **Computing the Dedekind different of smooth schemes and applications, Le Ngoc Long**
16:30 p.m. – 17:00 p.m. **Petroula Dospra, Dimitrios Poulakis** **Efficient algorithms for special roots of quaternion polynomials**
17:00 p.m. – 17:30 p.m. **Low autocorrelation binary sequences (LABS), Ilias Kotsireas**
17:30 p.m. – 18:00 p.m. **Kähler differential algebras for 0-dimensional schemes, Khanh Linh Tran**

Tuesday, June 27, 2017
8:30 a.m. – 9:30 a.m. **Track 4: Design Theory** **Track 4 Chairs: Lucia Moura (Canada), Dimitris Simos (Austria)** **Track 4: Invited Speaker** **Charles J. Colbourn (Arizona State University, USA)** **Computational and Recursive Constructions of Perfect Hash Families**
9:30 a.m. – 10:00 a.m **AG Codes, t-designs and Partition Sets , Cristina Marinez, Alberto Besana**
10:00 a.m. – 10:30 a.m **Covering Arrays as Set Covers , Ludwig Kampel, Bernhard Garn, Dimitris E. Simos**
10:30 a.m. – 11:00 a.m **Kochen-Specker Sets and Hadamard Matrices , Petr Lisonek**
11:00 a.m. – 11:30 a.m COFFEE BREAK
11:30 a.m. – 12:00 p.m **Number of t-tuples in arrays from LFSRs** **Daniel Panario, Brett Stevens, Georgios Tzanakis**
12:00 p.m. – 12:30 p.m **Disjoint q-Steiner systems in dimension 13, Michael Braun, Alfred Wassermann**
12:30 p.m. – 13:00 p.m **New Constant Weight Codes and Packing Numbers, Iliya Bluskov**
13:00 p.m. – 13:30 p.m **The Lovasz Local Lemma and Variable Strength Covering Arrays** **Lucia Moura, Sebastian Raaphorst, Brett Steven**
14:00 – 18:00 Conference Excursion, Ancient Messini Archaeological Site
19:30 – 22:00 Conference Banquet, Hotel Elite Conference Center

Wednesday, June 28, 2017
8:30 a.m. – 9:30 a.m. **Track 2: Cryptography and Coding Theory** **Track 2: Chairs: Stephane Ballet (France), Dimitrios Poulakis (Greece), Robert Rolland (France)** **Track 2: Invited Speaker** **Claude Carlet (Université Paris 8, France)** **Boolean functions with constrained inputs and the cryptosystem FLIP**
9:30 a.m. – 10:00 a.m. **A topological approach to network coding, Cristina Martinez, Alberto Besana**
10:00 a.m. – 10:30 a.m. **Pairing-Friendly Elliptic Curves Resistant to TNFS Attacks** **Georgios Fotiadis and Elisavet Konstantinou**
10:30 a.m. – 11:00 a.m. **Collaborative Multi-Authority Key-Policy Attribute-Based Encryption for Shorter Keys &Parameters** **Riccardo Longo, Chiara Marcolla, Massimiliano Sala**
11:00 a.m. – 11:30 a.m. COFFEE BREAK
11:30 a.m. – 12:00 p.m. Approximation of Differential Equations of Chaotic Attractors: Numerical Method as Encryption Key Field, Hana Ali-Pacha, Naima Hadj-Said, Adda Ali-Pacha
12:00 p.m. – 12:30 p.m. Conditional Blind Signatures **Alexandros Zacharakis, Panagiotis Grontas, Aris Pagourtzis**
12:30 p.m. – 13:00 p.m. Hash Function Design for Cloud Storage Data Auditing **Nikolaos Doukas, Oleksandr P. Markovskyi, Nikolaos G. Bardis**
13:00 p.m. – 13:30 p.m. Method for Accelerated Zero-Knowledge Identification of Remote Users based on Standard Block Ciphers, Nikolaos G. Bardis, Oleksandr P. Markovskyi, Nikolaos Doukas
13:30 p.m. – 14:00 p.m. Determining Whether a Given Block Cipher is a Permutation of Another Given Block Cipher a Problem in Intellectual Property, Gregory V. Bard
14:00 p.m. – 15:00 p.m. LUNCH BREAK
15:00 p.m. – 16:00 p.m. **Track 1: Automata Theory and Logic** **Track 1 Chair: Manfred Droste (Germany)** **Track 1: Invited Speaker** **Heiko Vogler (TU Dresden, Germany)** **Parsing of Natural Languages**
16:00 p.m. – 16:30 p.m. **Languages and formations generated by D_4 and Q_8, Jean-Éric Pin and Xaro Soler-Escrivà**
16:30 p.m. – 17:00 p.m. **Stefan Stanimirovic, Miroslav Ciric, J. Ignjatovic** **An improvement of the determinization of fuzzy finite automata via factorization of fuzzy states**
17:00 p.m. – 17:30 p.m. **Syntactic structures of regular languages, Ondrej Klima, Libor Polak**
17:30 p.m. – 18:00 p.m. **Pascal Caron, Jean-Gabriel Luque, Bruno Patrou** **Improving witnesses for state complexity of catenation combined with boolean operations**