Scientific program

The conference room is at the « cadran solaire ».

Informations

- Breakfast : from 07:15 to 09:15
- Lunch : from 12:15 to 13:15
- Dinner : from 19:30 to 20:15

Social events

- **Monday, June 9, 2014**
  18:45: welcome cocktail at the « Théâtre de verdure »
- **Wednesday, June 11, 2014**
  Afternoon - Social event: Nautic activities or Mountain bike
- **Thursday, June 12, 2014**
  22:00: « Le cadran lunaire »

Scientific committee

- **Aubry Yves**, IMATH/I2M, University of Toulon, France
- **Blondeau Céline**, Aalto University, Finland
- **Daemen Joan**, STMicroElectronics, Belgium
- **Didier Laurent-Stéphane**, IMATH, University of Toulon, France
- **Imbert Laurent**, LIRMM, University of Montpellier, France
- **Joye Marc**, Technicolor, Paris, France
- **Kohel David**, I2M, Aix-Marseille University, France
- **Laguillaumie Fabien**, University of Lyon, France
- **Langevin Philippe**, IMATH, University of Toulon, France
- **Leander Gregor**, Technical University of Denmark, Denmark
- **Lercier Reynald**, University of Rennes 1, France
- **Liardet Pierre-Yvan**, STMicroelectronics, France
- **Lubicz David**, CELAR, University of Rennes 1, France
- **Poulakis Dimitris**, University of Thessaloniki, Greece
- **Rolland Robert**, AcrypTA & eRISCS, France
- **Ritzenthaler Christophe**, IRMAR, University of Rennes, France
- **Sendrier Nicolas**, INRIA Rocquencourt, France
- **Tillich Jean-Pierre**, INRIA, Rocquencourt, France
- **Véron Pascal**, IMATH, University of Toulon, France

Yet Another Conference on Cryptography (June 9-13, 2014) is an international conference organized every two years by the « Institut de Mathématiques de Toulon » (IMATH, Toulon University, France).

The 7th edition is organized with the « Institut de Mathématiques de Marseille » (I2M, Aix-Marseille University).

Its main goal is to bring together industrialists and researchers around the following topics: cryptography, coding theory, computer arithmetic, number theory and algebraic geometry over finite fields.

The conference is sponsored by the « Université de Toulon », by the « Institut de Mathématiques de Toulon », by the « Institut de Mathématiques de Marseille », by the « Labex Archimède », by the FRUMAM (« Fédération de Recherche des Unités de Mathématiques de Marseille ») and by the « Axe Information de l'Université de Toulon ».

Website

- http://yacc.univ-tln.fr

Partners

INSTITUT de MATHÉMATIQUES de MARSEILLE

Labex Archimède

UNIVERSITÉ DE TOULON

AXE DE RECHERCHE UTLN Information

YACC 14

Yet Another Conference on Cryptography

Porquerolles, France june 9-13 2014

Invited speakers

- **Jean-Claude BAJARD (University of Paris 6, France)**
- **Daniel J. KATZ (California State University, Northridge, USA)**
- **Ruud PELLIKAAN (Eindhoven University of Technology, the Netherlands)**
- **Benjamin SMITH (Ecole Polytechnique, Paris, France)**
- **Jean-Pierre TILLICH (INRIA, Rocquencourt, France)**

Schedule Yacc'2014

All talks take place at « Cadran solaire ».

Monday, June 9, 2014

- 14:00: Departure of the Special Bus « YACC'2014 », from the Toulon bus station (nearby railway station) to « La Tour Fondue » Harbour
- 15:00: Departure of the Special Boat « YACC'2014 » to Porquerolles Island
- 15:30: Hotel Check In at the IGESA « Accueil »
- 16:30: Conference registration at the Conference Room « Le cadran solaire »
- 16:55: Opening
- 17:00: **Jean-Pierre Tillich** « Recent attacks on McEliece schemes based on Goppa codes »
- 18:00: **Alexis Bonnecaze** and **Robert Rolland** « Collecting Data while Preserving Individuals' Privacy: A Case Study »
- 18:45: Welcome cocktail
- 19:45: Dinner
- 22:00: GOT-S04-E10

Tuesday, June 10, 2014

- 9:30: **Jean-Claude Bajard** « Useful Systems of Representation for Cryptographic Implementations »
- 10:30: Coffee break
- 11:00: **Emanuele Bellini** « Yet another algorithm to compute the nonlinearity of a Boolean function »
- 11:30: **François Rodier** « Asymptotic nonlinearity of Boolean functions »
- 12:15: Lunch
- 15:00: **Ruud Pellikaan** « Public key cryptosystems based on algebraic geometry codes »
- 16:00: Coffee break
- 16:30: **Iaria Cardinali** and **Luca Giuzzi** « Polar Grassmann codes of orthogonal type »
- 17:00: **Grigory Kabatyanskiy** and **Valery Lomakov** « On Optimal Codes for Noisy Syndrome Decoding »
- 17:30: **Serhii Dyshko** « General isometries of codes »
- 18:00: **Regis Blache** « Questions about the divisibility of exponential sums, Fourier coefficients and weight of codes »
- 19:30: Dinner

Wednesday, June 11, 2014

- 9:30: **Daniel J. Katz** « Public key cryptosystems based on algebraic geometry codes »
- 10:30: Coffee break
- 10:45: **Yves Aubry** and **Annamaria Iezzi** « On the maximal number of points on singular curves over finite fields »
- 11:15: **Marc Joye** « Inversion-Free Arithmetic on Elliptic Curves Through Isomorphisms »
- 11:45: **Daniel Loebenberger** and **Michael Nüsken** « A family of 6-to-4-bit S-boxes with large linear branch number »
- 12:15: Lunch
- Afternoon - Social event: Nautic activities or Mountain bike
- 19:30: Dinner

Thursday, June 12, 2014

- 9:30: **Fabien Laguillaumie** « Lattice-Based Group Signatures with Logarithmic Signature Size »
- 10:30: Coffee break
- 11:00: **Franca Marinelli**, **Riccardo Aragona**, **Chiara Marcolla** and **Massimiliano Sala** « Some security bounds for the DGHV scheme »
- 11:30: **Dimitrios Poulakis** « A New Lattice Attack on DSA Schemes »
- 12:15: Lunch
- 15:00: **Ben Smith** « Compact Diffie-Hellman key exchange with efficient endomorphisms »
- 16:00: Coffee break
- 16:30: **Pierre-Alain Fouque**, **Antoine Joux** and **Chrysanthi Mavromati** « Multi-user collisions: Applications to Discrete Logarithm, Even-Mansour and Prince »
- 17:00: **Cécile Pierrot** and **Razvan Barbulescu** « The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields »
- 17:30: **Pietro Peterlongo**, **Claudia Tinirello** and **Massimiliano Sala** « Low-Weight Common Multiples of Binary Primitive Polynomials through Discrete Logarithms »
- 19:30 Conference Dinner
- 22:00 « Le cadran lunaire »

Friday, June 13, 2014

- 9h30: **Elena Andreeva** « Authenticated Encryption Security in Light of the Ongoing CAESAR Competition »
- 10:30: Coffee break
- 11:00: **Aysajan Abidin** and **Aikaterini Mitrokotsa** « A Privacy-Preserving Biometric Authentication Protocol Revisited »
- 11:30: **Kévin Atighehchi**, **Alexis Bonnecaze** and **Traian Muntean** « Behavior-driven authenticated data structure »
- 12:15: Lunch
- 14:30: Departure from IGESA
- 15:00: Departure of the Special Boat « YACC'2014 »
- 15:30: Departure of the Special Bus « YACC'2014 » from « La Tour Fondue » toward Toulon Bus Station
- 16:15: Arrival of the Special Bus at Toulon Bus Station.