Axe Information

Laboratoire LSIS
Laboratoire IMATH

Comité d'organisation

Pr. Hervé GLOTIN • glotin@univ-tln.fr
Pr. Laurent-Stéphane DIDIER • didier@univ-tln.fr

8es journées scientifiques

la RECHERCHE à l'Université

PALAIS NEPTUNE
TOULON **Entrée libre**
http://neptune2014.univ-tln.fr

8es journées scientifiques

la RECHERCHE à l'Université

Calcul Haute Performance : de la cryptanalyse aux masses de données scientifiques

Mardi 15 avril
Salle Jules Verne

Région PACA
Var Conseil Général
Toulon Provence Méditerranée
Toulon Port du Levant

UNIVERSITÉ DE TOULON

14h30 Scattering-based models for high-dimensional classification
Guy WOLF - DI ENS Ulm Paris

15h30 Masse de données bioacoustiques : codage et indexation à l'échelle
Hervé GLOTIN, Randall BALESTRIERO, CNRS LSIS UTLN & IUF

16h Discrete logarithm in GF(2^809) with FFS : an illustration of the use of HPC in cryptanalysis
Cyril BOUVIER - INRIA Nancy

17h Cryptanalyse du problème SD sur GPU
Pascal VÉRON, *Valentine MALYI, Laurent-Stéphane DIDIER,* IMATH UTLN

15 Mardi
avril 2014

'Scattering-based models for high-dimensional classification'

We present the recent Scattering methodology for classification and prediction. This methodology is based on the Scattering transform, which provides representations that are stable to deformations. The Scattering transform uses a convolutive network of Wavelet and modulus operations for building nonlinear invariants in data. Such invariants are crucial for high-dimensional classification tasks, where raw data representations do not provide meaningful similarities or distances.
As a particular case, we will examine the problem of blind source separation of pitched harmonic signals. In this application, the scattering methodology is used to perform slow learning by extracting slow changing components from the input signal, and defining a first-order prediction model for the harmonic structure of the separated sources. Then, the classification of the sources in the input mixed signal is done by minimizing the prediction error, without requiring pairwise relations between time frames or frequency bands which is efficient for big data processing.

'Discrete logarithm in GF(2^809) with FFS : an illustration of the use of HPC in cryptanalysis'

The year 2013 has seen several major complexity advances for the discrete logarithm problem in multiplicative groups of small-characteristic finite fields. These outmatch, asymptotically, the Function Field Sieve (FFS) approach, which was so far the most efficient algorithm known for this task. Yet, on the practical side, it is not clear whether the new algorithms are uniformly better than FFS.
This article presents the state of the art with regard to the FFS algorithm, and reports data from a record-sized discrete logarithm computation in a prime-degree extension field.