Visite du LORIA, 30 Novembre 2015

9:30 - 10:00	Accueil – Présentation du LORIA			
10:15 - 11:15	A1 J.Y. Marion	B1 V. Cortier	C1 M. Hoyrup	D1 P. Zimmermann
11:15 - 11:30	Pause Café			
11:30 - 12:30	A2 S. Lefebvre	B2 S. Perdrix	C2 J.B. Mouret	D2 E. Vincent S. Ouni
12:30 - 13:45	Pause déjeuner			
13:45 - 14:45	A3 S. Kremer	B3 J. Blanchette M. Duflot S. Merz	C3 D. Ritchie	D3 O. Devillers M. Teillaud
14:45 - 15:45	A4 P. Gaudry	B4 E. Vincent S. Ouni	C4 J. Blanchette M. Duflot S. Merz	D4 M. Couceiro C. Raïssi
15:45 - 16:00	Pause Café			
16:00 - 17:00	A5 B. Levy	B5 D. Ritchie	C5 J.B. Mouret	D5 O. Devillers M. Teillaud

Créneau 1 : 10:15 - 11:15

A1 Jean-Yves Marion. ***Virologie.***
En 30 minutes, j'exposerai les différents défis actuels qui concernent les codes malveillants (virus, vers, botnet, ...). On verra que les questions pratiques soulèvent des questions plus fondamentales et théoriques.

B1 Véronique Cortier. ***Vote électronique.***
Le vote électronique soulève de nombreux problèmes de recherche. Qu'est-ce qu'un bon système de vote électronique ? Est-ce réalisable ? Comment analyser un système de vote ? Nous aborderons ces questions au cours de l'exposé et nous montrerons comment les techniques d'analyse formelle développées dans l'équipe Cassis permettent d'étudier ces protocoles.

C1 Mathieu Hoyrup. ***Lire un programme ou l'exécuter : quelle différence ?***
Que peut-on savoir d'une fonction si elle nous est présentée :
- sous forme d'un programme calculant cette fonction,
- sous forme d'une boîte noire permettant de connaître les valeurs de cette fonction sur toutes les entrées.

Disposer d'un programme donne au moins autant d'information qu'avoir accès à la boîte noire. Cela donne-t-il plus d'information ? Dans ce cas, quel type d'information ? Cette question est un des problèmes les plus fondamentaux de l'informatique théorique et a donné lieu à de nombreux travaux, à commencer par ceux de Turing. Je présenterai les résultats historiques ainsi que les développements récents. Le domaine de recherche est la théorie de la calculabilité.

D1 Paul Zimmermann. ***Casser RSA avec CADO-NFS.***
Le logiciel CADO-NFS (http://cado-nfs.gforge.inria.fr/) implante l'algorithme du crible algébrique, qui a notamment été utilisé pour casser le challenge RSA-768. L'équipe Caramel a pour objectif de factoriser RSA-1024 avec CADO-NFS. Il reste à résoudre quelques défis pour y arriver...

Créneau 2 : 11:30 - 12:30

A2 Sylvain Lefebvre. ***Modélisation de structures complexes par l'exemple pour la fabrication additive.***
Nous nous intéressons à la génération automatique de structures complexes pour la fabrication additive (e.g. motifs entrelacés, treillis). Ces structures sont difficiles à créer manuellement car elles sont à la fois très détaillées mais doivent aussi respecter des contraintes mécaniques et géométriques strictes. Je présenterai plusieurs travaux récents qui permettent de générer automatiquement des telles structures à partir d'exemples.

B2 Simon Perdrix. ***Informatique Quantique.***
Des phénomènes mis en évidence par la physique quantique dans le comportement des particules élémentaires sont désormais considérés sous l'angle de leur exploitation pour représenter, traiter et communiquer l'information. Des résultats algorithmiques (algorithme de factorisation de Shor, algorithme de recherche de Grover), cryptographiques (distribution quantique de clés BB84, téléportation) et des avancées expérimentales soulignent l'intérêt d'un fondement quantique des sciences de l'information. Nous présenterons ce domaine de recherche notamment à travers les activités sur ce sujet de l'équipe Carte.

C2 Jean-Baptiste Mouret. ***Des robots qui s'adaptent comme des animaux.*** **(idem C5)**
Cet atelier sera composé d'un exposé (environ 45 minutes), suivi d'une visite de notre salle expérimentale robotique. L'exposé portera sur le sujet suivant. Après 50 ans de recherche en robotique, nous savons maintenant fabriquer des robots qui sont très efficace pour des tâches spécifiques et répétitives, mais on ne sait toujours pas comment le rendre capables d'opérer en dehors des environnements contrôlés des usines. C'est parce que les robots industriels et les robots "pour le monde réel" demandent des théories et des hypothèses fondamentalement différentes. Dans nos travaux, nous faisons l'hypothèse que les robots pour le monde réel doivent s'adapter comme des animaux: grace à un processus d'apprentissage par essai-erreur guidé par de bonnes intuitions, qui sont elles-mêmes le résultat de milliards d'années d'évolution et d'années d'expérience. Nous décrirons nos derniers résultats qui permettent à un robot marcheur de s'adapter à des pannes non anticipée (e.g. la perte d'une patte) par essai-erreur en moins de 2 minutes. La visite portera sur les robots hexapodes de notre groupe ansi que sur l'infrastructure logicielle et matérielle utilisée dans les expériences.

D2 Emmanuel Vincent & Slim Ouni. ***Traitement de la parole acoustique-visuelle et de la musique.*** **(idem B4)**

Cet atelier se focalise sur deux défis de traitement des signaux audio et audiovisuels: la séparation de sources et la synthèse de la parole audiovisuelle. La séparation de sources vise à extraire le signal d'un locuteur ou d'un instrument de musique d'un enregistrement contenant d'autres sources sonores. Elle repose sur l'analyse temps-fréquence et l'apprentissage automatique et permet d'améliorer la qualité des communications téléphoniques et de la commande vocale ou de remixer la musique, entre autres applications. La synthèse de la parole audiovisuelle porte sur l'animation réaliste d'une tête parlante virtuelle (avatar) qui prend en compte les mécanismes d'articulation de la parole (les mouvements des lèvres, de la langue et de la mâchoire). Dans nos travaux, on utilise des outils de capture de mouvement pour le visage (techniques de stéréovision : avec et sans capteurs) et pour les mouvements des lèvres et de la langue (technique d'électromagnétographie). Ces données permettent de développer des algorithmes d'animation du visage synchrone avec la parole.

Créneau 3 : 13:45 - 14:45

A3 Steve Kremer. ***Vérification de protocoles cryptographiques.***

Les protocoles cryptographiques sont des programmes distribués qui utilisent des primitives cryptographiques, telles que le chiffrement, pour assurer des propriétés de sécurité, comme par exemple la confidentialité. Cependant, même sans casser la cryptographie, il est souvent possible de déjouer les objectifs de ces protocoles. Nous allons voir comment utiliser des outils issus de la logique pour trouver des failles, ou prouver leur absence, dans ces protocoles.

B3 Jasmin Blanchette, Marie Duflot & Stephan Merz. ***Dompter des algorithmes avec de la logique.*** **(idem C4)**

Nous étudions comment des techniques fondées sur la logique formelle peuvent aider à raisonner sur les algorithmes et systèmes informatiques, en particulier distribués. Différentes techniques interviennent, selon qu'il s'agit de trouver des erreurs ("model checking") ou de démontrer formellement la correction par des outils de preuve automatique ou interactive. Pour les plus grands systèmes, mais aussi pour étudier des aspects quantitatifs (temps de réponse, ressources en mémoire ou réseau), il est utile de combiner logique et statistiques. Nous allons présenter les bases de nos travaux, ainsi que des idées pour d'éventuels stages.

C3 Dave Ritchie. ***The "Capsid" Team - Developing Computational Algorithms for Protein Structures and their Interactions .*** **(idem B5)**

Capsid is a new research team at Inria Nancy / LORIA, which was created in 2015. The main aim of the team is to work on problems in structural biology. This work involves developing efficient ways to represent and compare large three-dimensional bio-molecules such as proteins. For example, if we have two different but related proteins, how can we measure how similar they are? If we know from biology that two or more proteins can fit together (or "dock") to form a complex, how can we simulate this in a computer? In this workshop, I will talk about some of the problems that the Capsid team are working on, and I will demonstrate some of our software for comparing different protein structures and for docking two or more proteins to make models of large 3D protein complexes. The presentation will be in English.

D3 Olivier Devillers & Monique Teillaud. ***L'ordinateur géomètre.*** **(idem D5)**

Les membres du projet Vegas présenteront des démos autour de leur sujet de recherche. - Dessiner des courbes sans confondre proximité et intersections - Des géométries exotiques pour déplier le tore ou le double-tore - Faire un compromis entre le cas le pire et le complétement aléatoire.

Créneau 4 : 14:45 - 15:45

A4 Pierrick Gaudry. ***Le logarithme discret, de la théorie des nombres à la sécurité d'internet.***

Le problème du logarithme discret est au cœur de nombreux algorithmes utilisés pour sécuriser les communications. Le meilleur algorithme connu pour attaquer ce problème, le crible algébrique, doit être étudié en profondeur, aussi bien en théorie qu'en pratique afin de régler au mieux les paramètres des protocoles cryptographiques. Nous donnerons un aperçu du crible algébrique et raconterons comment une de ses particularités est à la base de la découverte récente d'une faille importante dans la mise en œuvre du protocole TLS.

B4 Emmanuel Vincent & Slim Ouni. ***Traitement de la parole acoustique-visuelle et de la musique.*** **(idem D2)**

C4 Jasmin Blanchette, Marie Duflot & Stephan Merz. ***Dompter des algorithmes avec de la logique.*** **(idem B3)**

D4 Miguel Couceiro & Chedy Raïssi. ***Recherche de motifs et théorie de l'agrégation en analyse de données***

Créneau 5 : 16:00 - 17:00

A5 Bruno Levy. ***Simulation numérique, lois de conservation et transport optimal.***

La simulation numérique permet de reproduire dans un ordinateur le comportement de différentes lois physiques, modélisées par des equations aux dérivées partielles. L'une des difficultés est de s'assurer que les lois de conservation soit bien respectées par ces simulations numériques. Dans certains cas, par exemple le problème de reconstruction de l'état de l'univers peu après le big-bang [1], l'expression de ces lois de conservation permet d'établir des relations intéressantes avec d'autres domaines des mathématiques, tels que la théorie du transport optimal [1,2]. En termes informatique, ceci conduit à de nouveaux schémas numériques, faisant appels à une forte composante géométrique [3,4].

[1] Reconstruction of the early universe as a convex optimization problem, Brenier, Frisch et.al, 2003, http://arxiv.org/abs/astro-ph/0304214
[2] Optimal Transport, Old and New, Villani, 2008
[3] A multiscale approach to optimal transport, Mérigot, Symp. on Geometry Processing, 2011
[4] A numerical algorithm for L2 optimal transport in 3D, Lévy, Mathematical Modeling and Analysis, 2015, http://arxiv.org/abs/1409.1279

Video: Semi-discrete Optimal Transport and some of its application, summer school on geometric measure theory, `https://www.youtube.com/watch?v=qki-Z68Yqno&index=32&list=PL0E0n75oNCDleNYItxl93ckbQjSOkCXtQ`

B5 Dave Ritchie. ***The "Capsid" Team - Developing Computational Algorithms for Protein Structures and their Interactions .*** **(idem C3)**

C5 Jean-Baptiste Mouret. ***Des robots qui s'adaptent comme des animaux.*** **(idem C2)**

D5 Olivier Devillers & Monique Teillaud. ***L'ordinateur géomètre.*** **(idem D3)**