RAIM 2012: LE PROGRAMME

Mercredi 20 juin

13h00 Accueil des participants

14h00 **SESSION CALCUL À HAUTE PERFORMANCE :**
– Fabienne JÉZÉQUEL (LIP6, Paris)

14h00 Bernard GOOSSENS (DALI, Perpignan)
Parallélisme dynamique

15h30 M. MARIN (DALI)
Implémentation of Rootfix and Leaffix primitive in OpenCL.

16h00 Pause

16h30 Édouard CANOT (SAGE, IRISA)
Solveur DAE et Calcul symbolique.

17h00 Mourad GOUICEM.
Correctly rounding transcendental functions with GPUs

17h30 **SESSION INTERVALLES :**
– Nathalie REVOL (LIP, ENS Lyon, Université de Lyon)

17h30 Philippe THÉVENY (LIP, ENS de Lyon, Université de Lyon)
Divers algorithmes de produits de matrices intervalles

18h00 Nathalie REVOL (INRIA, LIP, ENS de Lyon, Université de Lyon).
L'effort de normalisation IEEE-1788 de l'arithmétique par intervalles

18h30 Dominique MICHELUCCI (LE2I, Dijon)
Problème de Bernstein; Calcul par intervalles et fractales

19h00 Fin de la première journée

Jeudi 21 juin

9h00 **SESSION ARITHMÉTIQUE INDUSTRIELLE :**
– Philippe LANGLOIS (DALI / LIRMM, Perpignan)
9h00 Nicolas BRUNIE (LIP, et société Kalray)
Unité virgule flottante dans un processeur actuel
9h30 Duco Van AMSTEL (LIP / ENS Lyon, et Kalray)
Implémentation bit-slice de l'AES et de
la multiplication de matrices dans GF(2)
10h00 Pause
10h30 Christophe DENIS (EDF R&D, Clamart).
Étude de la qualité numérique de codes numériques industriels
11h00 **OUVERTURE THÉMATIQUE:**
Arnaud TISSERAND (IRISA, Lannion)
Génération de nombres aléatoires "vrais" en matériel

12h00 Repas Montmuzard

14h00 **SESSION CRYPTOGRAPHIE :**
– Christophe NÈGRE (DALI / LIRMM, Perpignan).
14h00 Marine MINIER (INSA Lyon).
Les 10 ans de l'AES.
15h00 Thomas CHABRIER (IRISA, Lannion).
Protections arithmétiques contre certaines attaques
physiques de cryptosystème
Template attacks on hardware implementation of SD recoding for ECC
15h30 Thomas PLANTARD (Université de Wollongong)
Cryptographie sur les réseaux
16h00 Pause
16h30 Jérémy JEAN (ENS Paris), Thomas PEYRIN
et Maria NAYA-PLASENCIA.
Une attaque sur la fonction de hachage Grøstl.
17h00 Jean-Marc ROBERT (DALI / LIRMM, Perpignan).
Optimisations de l'implantation en C sur un processeur
Intel Core I7 de la multiplication scalaire sur
les courbes elliptiques binaires
17h30 **TABLE RONDE / ASSEMBLEE GENERALE DU GT**
18h00 Fin de la deuxième journée
Dîner à Dijon.

Vendredi 22 juin

8h15 **SESSION QUALITÉ NUMÉRIQUE :**
– Valérie MÉNISSIER-MORAIN (LIP6, Paris).

8h15 Andréas ENGE (INRIA, Bordeaux).
MPC, MPFRCX

9h15 Ioana PASCA (LIP, ENS Lyon, Université de Lyon.
Preuves formelles en Coq pour les modèles de Taylor

9h45 Pause

10h00 Christoph LAUTER et Valérie MÉNISSIER-MORAIN (LIP 6)
Sur la stabilité des modes d'arrondi.

10h30 Valérie MÉNISSIER-MORAIN.
Arithmétique compensée.

11h00 Laurent THÉVENOUX (DALI / LIRMM)
Transformation automatique de code pour optimiser la précision
et la vitesse des calculs en arithmétique flottante

11h30 Séthy MONTAN (EDF R&D, LIP6)
Une implémentation efficace de CADNA dans les BLAS:
exemple de la routine DgemmCADNA

12h00 Repas Montmuzard

13h30 **SESSION VIRGULE FIXE :**
– Laurent Stéphane DIDIER (LIP6, Paris)
et Daniel MÉNARD (ENSSAT, IRIS, Rennes)

13h30 Daniel MÉNARD (ENSSAT, IRIS, Rennes)
Evaluation des performances des systèmes en virgule fixe

14h00 Benoit LOPEZ
Schémas d'évaluation de produits scalaire en arithmétique virgule fixe,
application aux filtres IIR.

14h30 Amine NAJAHI
Synthesis of fixed-point programs based on instruction selection:
the case of polynomial evaluation

15h00 Clôture de RAIM 2012