DALI
Digits, architectures et logiciels informatiques

1 Présentation générale

L'équipe DALI[1] développe une thématique de recherche unifiée afin d'améliorer la qualité numérique et la haute performance des calculs. DALI permet l'interaction, rare en France au sein d'une même équipe, de chercheurs spécialisés en **micro-architecture** et en **arithmétique des ordinateurs**.

Côté performances, nos travaux portent sur l'exploitation du potentiel de calcul toujours croissant des processeurs : élargissement des chemins (micro-architecture vectorielle), multiplication des cœurs (parallélisme de tâches), augmentation du parallélisme d'instructions. Côté arithmétique, la qualité numérique des applications de calcul scientifique ou des applications embarquées dépend crucialement de la maîtrise des effets de la précision finie et de l'arithmétique flottante en particulier. Il s'agit de contrôler et certifier les calculs (algorithmes, codes) mais aussi d'optimiser la précision des traitements. De nombreux logiciels, scientifiques ou embarqués, nécessitent d'améliorer la qualité numérique sans pour autant sacrifier la rapidité d'exécution ou le coût énergétique. Ainsi se rejoignent amélioration de la performance et de la qualité numérique.

L'équipe est active et bien visible dans les communautés nationales scientifiques de l'**informatique mathématique** et de l'**architecture des ordinateurs**, et est très régulièrement impliquée dans les structures d'animation de la recherche de ces domaines. Les doctorants issus de DALI sont globalement recrutés avec succès dans des structures de recherche publiques ou privées, en France ou à l'étranger.

L'équipe, composée d'enseignants-chercheurs de l'Université de Perpignan Via Domitia, est localisée sur la campus de Perpignan situé à 2 heures de transport du laboratoire. Elle relève de l'école doctorale de l'UPVD (ED305 énergie et environnement) et de ses programmes d'appui à la recherche (budget récurrent, appels BQR et PEPS).

2 Evolution de l'équipe

Composition au 1er janvier 2017 :
- 6 permanents : 2 PR1 (B. Goossens, Ph. Langlois), 2 MCF HDR (D. Defour, Ch. Negre), 2 MCF (D. Parello, G. Revy)
- 1 assistante (S. Munoz, 50%)
- 1 personnel statutaire chercheur associé (J.M. Robert, professeur agrégé, Béziers)
- 1 post-doc (R. Nheili, ATER à 50%)
- 3 doctorants (C. Chohra, H. de Lassus Saint-Geniès, K. Porada)

1. `http:webdali.univ-perp.fr`

Aucune arrivée de nouveau chercheur permanent. Un départ de MCF HDR et 1.5 doctorant en 2015. Accueil d'un ATER par an. Sur la période concernée, les deux premières soutenances d'HDR de membres recrutés comme MCF dans l'équipe ont eu lieu (2014, 2016). La bonne fréquence de soutenance des doctorats et de leur durée de préparation ont été maintenues : 5 thèses soutenues dans la période et préparées en 39.4 mois en moyenne. Mentionnons deux thèses arrêtées en 2016 : l'un sur abandon du doctorant, l'autre sur décision de l'école doctorale après avis du comité de suivi de thèse.

La direction d'équipe a été renouvelée en 2015 suite au départ (inattendu) du précédent responsable (M. Martel).

3 Organisation et vie de l'équipe

DALI a maintenu son positionnement scientifique resserré autour de la performance et de la précision des calculs, tout en satisfaisant les besoins d'enseignement d'une petite université pluridisciplinaire. DALI a incité au dynamisme scientifique des membres de l'équipe et en particulier chacun d'entre eux a co-encadré au moins une thèse dans la période. La vie scientifique profite de l'unité de lieu, de nouveaux locaux depuis 2013, d'un séminaire et de réunions d'équipe réguliers. Sur la période, ces activités ont été renforcées par la mise en place de « journées scientifiques hors labo » où la totalité des membres ont échangé autour de leurs travaux, ainsi que par l'intervention régulière des doctorants en séminaire. Ce dernier évolue vers des interventions par visio-conférence pour compenser le coût élevé des déplacements vers Perpignan. L'intégration au LIRMM constitue depuis 2011 une ouverture intéressante : travaux communs de l'ANR PAVOIS et du projet européen Mont-Blanc2, implication dans la vie de la plateforme HPC@LR, participation à la mise en place régionale de l'ISN, etc.

4 Activités scientifiques

L'unité thématique des travaux de recherche pour améliorer la qualité numérique et la performance des calculs est une des forces de l'équipe DALI.

L'amélioration de la performance des calculs est étroitement liée aux améliorations apportées aux micro-architectures. Celle-ci est réalisée suivant plusieurs directions, par élargissement des chemins (micro-architecture vectorielle), multiplication des cœurs (parallélisme de tâches), ou encore augmentation du parallélisme d'instructions (ILP). La qualité numérique des applications de calcul scientifique ou la validation du fonctionnement d'applications embarquées critiques dépendent crucialement de la maîtrise des effets de la précision finie des calculs — et de l'arithmétique flottante en particulier. Il s'agit alors de contrôler et valider les calculs (algorithmes, codes) mais aussi d'améliorer et optimiser la précision des calculs et des résultats.

Les travaux développés sur la période 2013-2016 sont organisés autour de 4 actions de recherche.

Action 1. Analyse du potentiel de parallélisme et amélioration des performances.

Action 2. Meilleure exploitation des nouvelles architectures multicœurs.

Action 3. Implantation sûre et efficace de protocoles cryptographiques.

Action 4. Algorithmes et outils pour une meilleure qualité numérique des calculs.

4.1 Action 1 : autour du logiciel PerPI

Notre approche de la performance des calculs s'appuie sur le parallélisme d'instructions (ILP). Le logiciel PerPI (Performance et Parallélisme d'Instructions) mesure le potentiel d'ILP. Les instructions indépendantes sont considérées comme parallélisables quel que soit leur éloignement mutuel [1]. On peut ainsi exhiber tout le parallélisme disponible, où qu'il se situe dans le flot d'exécution. PerPI nous permet de comprendre où sont les freins au parallélisme — ils viennent plus de l'architecture que de l'algorithme ou du programme — et déceler quantité de sources de parallélisme, notamment dans les fonctions une fois enlevée la sérialisation par la pile, et dans les boucles une fois transformées en fonctions récursives. On peut aussi quantifier l'augmentation de l'ILP par diverses transformations de programmes et en déduire une nouvelle forme de programmation plus propice à la parallélisation matérielle.

Le calcul HPC s'appuie sur des bibliothèques mathématiques qui doivent être précises et performantes. Au niveau de l'algorithmique pour l'arithmétique à virgule flottante et en liaison avec l'action 4, nous avons introduit des algorithmes compensés qui produisent des résultats arbitrairement précis et validés, qui bénéficient de vitesse d'exécution supérieure aux solutions existantes. Nous avons étudié et expliqué cette efficacité. PerPI permet de caractériser le potentiel de performance des algorithmes numériques, et ce de manière reproductible contrairement aux approches classiques fondées sur le décompte des opérations ou des cycles machines.

4.2 Action 2 : architectures multicœurs

L'arrivée des architectures à plusieurs dizaines ou millier de cœurs avec les GPU, les unités multi- et many-coeurs, a révolutionné le monde du HPC. S'il est désormais possible d'effectuer plus de calcul et plus vite, de nouvelles contraintes apparaissent aux niveaux matériel et logiciel pour offrir des garanties sur les résultats produits. Ces contraintes sont de nature architecturale ou logicielle.

Parmi les contraintes architecturales, nous avons poursuivi nos travaux liés à l'étude du comportement des GPU. Premièrement, nous avons constaté, que les GPU étaient aussi sensibles que les autres architectures aux vieillissements des circuits mais qu'ils présentaient certaines singularités liées à leur structuration interne du calcul. En exploitant ces singularités nous avons proposé des solutions permettant de fiabiliser les calculs sur des architectures many-coeurs ayant des unités défectueuses [ART.5]. Deuxièmement, nous avons initié un travail sur l'utilité d'intégrer des opérateurs spécialisés paramétrables. Cette démarche est justifiée au niveau industriel par exemple par le rachat d'Altera par Intel.

Concernant les contraintes logicielles, la récente multiplication des unités de calcul flottantes a conduit de nombreux développeur à utiliser des algorithmes parallèles pouvant générer des problèmes numériques. Nous avons par exemple analysé comment ces nouveaux algorithmes se comportent d'un point de vue numérique sur des applications concrètes comme le parcours de graphe dans le cas des smartgrids (thèse de M. Marin, 2014). Ces nouvelles architectures étant plus contraintes par le débit mémoire que par la capacité de calcul, il est désormais intéressant du point de vue du coût de considérer l'utilisation d'arithmétiques dites non-conventionnelles. Sur cet exercice nous avons donc proposé une bibliothèque d'arithmétique floue pour GPU afin de gérer les incertitudes de deuxième ordre [CACT.29, ART.3]. Dans ce cadre, nous avons aussi proposé des solutions au problème de la non-reproductibilité numérique des résultats liés à la non-associativité des opérations flottantes qui seront plus largement

présentées avec l'action 4.

4.3 Action 3 : protocoles cryptographiques

Les protocoles cryptographiques les plus populaires sont RSA et les différents protocoles basés sur les courbes elliptiques (ECC). Ces derniers ont gagné en attractivité dû à leurs tailles de clefs réduites et leurs nouvelles fonctionnalités provenant des couplages. Notre recherche consiste à proposer de nouvelles approches pour l'implantation sûre et efficace de protocoles cryptographiques RSA et ECC.

L'opération centrale des protocoles cryptographiques consiste en une séquence de multiplications et d'additions dans un corps ou un anneau finis. Pour améliorer l'efficacité de ces protocoles cryptographiques, nous avons proposé des améliorations des algorithmes pour la multiplications dans les corps binaires [ART.12, ART.9, ART.14, ART.13]. Nous avons aussi amélioré le calcul des opérations combinées AB, AC et $AB + CD$ en partageant certains calculs communs [CACT.21, CACT.38].

Durant la période, nous avons participé au projet ANR Pavois qui a financé la thèse de J-M. Robert (2012-2015). L'objectif de ce projet était de proposer de nouvelles protections contre les attaques à canaux cachés sur des implantations matérielles d'ECC. Ces attaques exploitent des fuites d'information que l'on peut extraire de la puissance consommée, du temps de calcul ou de l'émanation électromagnétique. Nous avons travaillé sur des algorithmes d'exponentiation ou de multiplication scalaire réguliers [ART.7, ART.1] pour assurer une protection contre des attaques Simple Power Analysis. Nous avons aussi travaillé sur la randomisation des opérations modulaires dans le système de représentation RNS [CACT.20] et en représentation classique [CACT.5]. Ces randomisations perturbent les calculs, ce qui permet de mieux masquer les opérations effectuées dans les mesures physiques.

4.4 Action 4 : pour une meilleure qualité numérique des calculs.

L'amélioration de la qualité numérique des calculs est étudiée selon deux angles : la synthèse de code et la reproductibilité numérique. La synthèse de code est motivée par la diversité des architectures matérielles actuelles, de leurs unités de calculs et des arithmétiques qu'elles supportent. Étant donné un problème numérique (expression mathématique, algorithme, code numérique pré-existant), nous souhaitons produire une implantation qui soit à la fois rapide, suffisamment précise et certifiée. Par ailleurs, l'utilisation massive du calcul parallèle (HPC) pour simuler numériquement des problèmes complexes a récemment fait émerger des cas de non-reproductibilité numérique de résultats : les exécutions successives d'une simulation retournent des résultats différents bien que les entrées et les schémas de résolution soient inchangés. Nous proposons des solutions algorithmiques et logicielles qui résolvent ce problème.

Sur la période concernée, l'activité de synthèse de code s'est développée autour de deux objectifs. Au niveau des briques numériques, e.g. fonctions élémentaires ou petits blocs d'algèbre linéaire, nous avons étendu le champ d'application de l'outil CGPE. Initialement destiné à la synthèse automatique de codes rapides et certifiés pour l'évaluation polynomiale en virgule fixe, l'outil CGPE permet aujourd'hui de produire des codes pour évaluer d'autres problèmes (e.g. sommation, produit scalaire), utilisant au mieux les instructions de l'architecture cible. CGPE peut maintenant produire automatiquement des programmes virgule fixe, rapides et certifiés, pour traiter des blocs numériques de plus haut niveau, comme la multiplication ou l'inversion de matrices [CACT.34, CACT.25]. Ces travaux ont

été réalisés dans le projet ANR DEFIS (2011-2015 et la thèse de A. Najahi (2014.Ils ont donné lieu au développement de l'outil FPLA. Pour la virgule flottante, nos travaux ont concerné l'amélioration de la précision à l'aide de transformations sans erreur. La thèse de L. Thévenoux (2014) fournit une infrastructure logicielle qui réalise une synthèse de codes avec compromis performance-précision. L'enjeu est de déterminer quelles parties de code transformer sans trop impacter les performances de l'application. Pour la virgule flottante, nous nous sommes également intéressés à la génération de codes pour l'évaluation de fonctions élémentaires (exponentielle, logarithme [CACT.7], trigonométriques, ...), et plus particulièrement à la prise en compte des contraintes architecturales lors du processus de génération. Par exemple une manière d'implanter ces fonctions mathématiques est d'utiliser une méthode à base de tables, qui stocke le résultat approché de ces fonctions pour un ensemble d'arguments bien choisis. Dans le cadre du projet ANR MetaLibm (2013-2017) et de la thèse de H. de Lassus Saint-Geniès, nous avons proposé une méthode qui permet de tabuler des valeurs exactes et ainsi, réduire la taille des tables et accélérer le processus d'évaluation [CACT.19, CACT.16].

La non-reproductibilité numérique du calcul parallèle remet en question la fiabilité et le degré de confiance des simulations numériques de nombreux domaines d'application industrielle (chimie, énergétique, ...) ou de recherche (études du climat, du système solaire, ...). Le débugage, le test, la validation ou la certification par des autorités de contrôle imposent de corriger ce comportement essentiellement causé par le non-déterminisme des exécutions parallèles (ordonnancement et réductions dynamiques), la non-associativité de l'addition de l'arithmétique flottante et la dépendance entre la propagation des erreurs d'arrondis générées et l'ordre des séquences de calcul [ART.10]. Nous appliquons le principe d'une augmentation ciblée de la précision des calculs qui soit suffisante à la reproductibilité numérique dans deux contextes différents.

Une première étape est de pouvoir disposer de BLAS parallèles, efficaces et numériquement reproductibles, ces dernières étant les briques de base optimisées de l'algèbre linéaire numérique. Deux directions ont été suivies. Nous participons au développement de la bibliothèque exBLAS [ART.6] qui cible plus particulièrement les architectures massivement parallèles (GPU, accélérateurs). Par ailleurs, des BLAS de niveaux 1 et 2, précises, reproductibles et performantes basées sur des algorithmes récents de sommation correctement arrondie sont aussi proposées dans la bibliothèque RARE-BLAS (thèse de C. Chohra) [CACT.8, CACT.2, CACT.3].

A large échelle ensuite, des techniques de compensation ont permis de retrouver la reproductibilité numérique des simulations par éléments finis du code d'hydrodynamique industrielle open source Telemac-Mascaret (thèse de R. Nheili, 2016) [CACT.15, CACT.18, CACT.4].

5 Faits marquants

5.1 Prix et distinctions

— Best Paper Session pour l'article *Power Flow analysis under uncertainty using Symmetric Fuzzy Arithmetic* à la conférence IEEE PES-GM 2014.
— Best Paper Award for GPU applications pour l'article *FuzzyGPU : a fuzzy arithmetic library for GPU*, à la conférence PDP 2014.

6 Rayonnement

6.1 Organisation d'événements

— Workshop *Numerical Reproducibility for High-Performance Computing*, 17th SIAM Conference on Parallel Processing for Scientific Computing, Paris (2016)
— Mini-symposium *Reproductibilité numérique*, congrès annuel SMAI, Seignosse (2013).
— Rencontres Arithmétique et Informatique Mathématique (RAIM'16)
— Ecole jeunes chercheurs du GDR Informatique Mathématique (EJCIM'13)

6.2 Comités de programme et activité éditoriale

— Comités de programme de conférences internationales et nationales
  — Membre des comités de programme des conférence PaCT (15,17), PDP (13, 14, ..., 17), MCSoc (15, 16, 17), HPCS (16, 17), PDCTA (17)
  — Membre des comités de programme de la conférence Compas (éditions 14, 15, ..., 17)
  — Présidence du track Archi de la conférence Compas 2016

— Activité éditoriale
  — Informatique-Mathématique : une photo en 2013, 2014, ..., 2017. Série publiée aux PUP puis CNRS Editions : création, édition du premier numéro, comité scientifique et éditorial.
  —)i(Interstices : comité éditorial.

6.3 Invitation

— Exposé invité du track Archi de la conférence Compas 2014, Neuchâtel (Suisse)

7 Valorisation et transfert

7.1 Valorisations contractuelles

Actility (2013-2014) Cette collaboration avec la société Actility concernait une étude de faisabilité sur les gains en performance des accélérateurs matériels de type GPU pour une application de calcul de l'état d'un réseau de distribution électrique.

L'objectif de cette étude de faisabilité était de rechercher et comparer diverses solutions liées à la problématique du contrôle d'admission au sein du logiciel DOME développé à UCLM avec pour objectif principal la performance. Cette performance était nécessaire afin d'accélérer les temps de simulation et pouvoir tendre vers des prises de décision en temps réel. Nous avons pour cela étudié l'ensemble de la chaîne logicielle en proposant d'utiliser des processeurs graphiques combinés à de nouveaux schémas algorithmiques.

3E (2015-2016) Cette collaboration avec la société 3E concernait l'exploitation par des techniques de datamining des données issues des réseaux de capteur que l'on trouve dans les centrales solaires photovoltaïques.

L'objectif de cette étude était de modéliser la performance des onduleurs photovoltaïques en fonction du temps, à partir des données de terrain. Les modèles visés ont facilité la détection des effets de vieillissement et permis de quantifier les pertes associées en permettant de prédire certaines pannes.

EDF R&D (2016-2017) Cette collaboration avec le LNHE et le Laboratoire National Saint-Venant (Chatou) concerne l'amélioration de la reproductibilité numérique de modules du code d'hydrodynamique open TELEMAC-MASCARET.

L'étude a pour objectif d'améliorer la reproductibilité numérique de ce code, et plus particulièrement le module d'hydrodynamique bidimensionnelle TELEMAC2D. Les sources de la non-reproductibilité numérique d'exécutions parallèles de simulations de référence (cas-test) inclues dans la distribution de TELEMAC2D ont d'abord identifiées. De nouvelles solutions algorithmiques qui améliorent la reproductibilité numérique de ces traitements dans un environnement de calcul parallèle ont été définies, implémentées et validées sur ces cas-tests. Ces solutions sont intégrées dans la distribution 2017 d open TELEMAC-MASCARET.

7.2 Expertises et transfert technologique

— Membre du Conseil d'Orientation Scientifiques, Techniques et Industriels de la région Languedoc-Roussillon Midi-Pyrénées (COSTI)

8 Collaborations

8.1 Projets collaboratifs

— ANR :
  — ANR INS DEFIS (2011-2015)
  — ANR INS CAFEIN (2012-2015)
  — ANR Pavois (2012-2015)
  — ANR MetaLibm (2014-2017)
— CNRS : PEPS QUARENUM (2013).

8.2 Autres collaborations

— University of Wollongong (Australie) : séjour de 10 mois en 2014-2015 d'un doctorant à l'Université de Wollongong financé par Thlexinoe. Séjour d'un mois de T. Plantard à DALI en 2015 aussi financé par Thelxinoe.
— University College Dublin : co-tutelle de la thèse de M. Marin (2012-2015)
— Département MIC (LIRMM) : co-direction (avec G. Sassatelli, département MIC) de la thèse de K. Porada sur l'évaluation d'un modèle de processeur parallélisant, projet européen MontBlanc2.

9 Production scientifique

9.1 Cinq publications majeures

— D. Defour and E. Petit. A software scheduling solution to avoid corrupted units on GPUs. *Journal of Parallel and Distributed Computing*, 90-91 :1–8, Apr. 2016.

Résumé : Les processeurs modernes sont de plus en plus sujets aux défaillances matérielles. Ces défaillances sont dues à différents facteurs liés à la tension, la fréquence ou le processus de gravure des transistors. Ces erreurs peuvent être permanentes, transitoires ou intermittentes. Leurs nombres et leurs fréquences d'apparitions augmentent avec le vieillissement des puces. Il est donc nécessaire de composer avec le fait qu'une architecture tel qu'un GPU à l'origine fiable, devienne non-fiable avec le temps. Nous avons proposé une solution logicielle (middleware) permettant de contenir le calcul sur les unités valides et éviter les unités problématiques en exploitant les spécificités du modèle de programmation des GPU.

— B. Goossens, D. Parello, K. Porada, and D. Rahmoune. Toward a Core Design to Distribute an Execution on a Many-Core Processor. In V. Malyshkin, editor, *PaCT : Parallel Computing Technologies*, volume LNCS of *Parallel Computing Technologies*, pages 390–404, Petrozavodsk, Russia, Aug. 2015. Springer International Publishing.

Résumé : L'article présente un modèle d'exécution parallèle et une conception de processeur à plusieurs coeurs pour exécuter des programmes C en parallèle. Le modèle construit automatiquement des sections parallèles d'instructions machine à partir de la trace d'exécution. Il parallèlise la lecture, le renommage, l'exécution et le retrait des instructions. La lecture d'instruction n'est pas basée sur un prédicteur de saut mais par un étage de lecture-décodage-et-exécution partielle capable de calculer en ordre la plupart des instructions de contrôle. Le mécanisme de renommage des registres de Tomasulo est étendu à la mémoire avec une technique permettant de faire correspondre les paires consommateur / producteur. Le tampon de réorganisation (ROB) est adapté pour permettre le retrait en parallèle des instructions. Le modèle est présenté sur un exemple de réduction de somme qui est également utilisé pour une évaluation analytique du potentiel de performance du modèle.

— P. Langlois, R. Nheili, and C. Denis. Recovering numerical reproducibility in hydrodynamic simulations. In *ARITH 23*, IEEE Symposium on Computer Arithmetic, Silicon Valley, Santa Clara, CA, United States, July 2016.

Résumé : Les simulations HPC souffrent de non-reproductibilité numérique à cause de faiblesses de l'arithmétique flottante. Des distributions différentes d'un calcul parallèle peuvent fournir des résultats numériques différents. Nous nous intéressons à des simulations d'hydrodynamique par éléments finis avec le logiciel openTelemac où le parallélisme repose sur de la décomposition de domaines. Une des étapes principales d'une telle simulation est la construction d'un sytème linéaire de grande taille, puis sa résolution. Ici l'étape de construction est basée sur un stockage élément-par-élément, et la résolution sur l'algorithme du gradient conjugué. Le parallélisme de sous-domaine est imbriqué dans ces étapes. Nous étudions pourquoi la reproductibilité numérique est perdue dans ce traitement et quelles opérations doivent être corrigées. Nous détaillons comment les techniques de compensation permettent d'obtenir une résolution numériquement reproductible. Nous illustrons cette approche en présentant une version reproductible pour un cas de simulation fourni avec la distribution du logiciel openTelemac.

— C. Negre and J.-M. Robert. New Parallel Approaches for Scalar Multiplication in Elliptic Curve over Fields of Small Characteristic. *IEEE Transactions on Computers*, 64(10) :2875–2890, Sept. 2015.

Résumé : Nous présentons deux nouvelles stratégies pour la mise en œuvre parallèle de la multiplication scalaire sur les courbes elliptiques. Nous introduisons d'abord une variante de la multiplication scalaire de Montgomery exploitant le halving de point sur $E(GF(2^m))$. Le Montgomery-halving peut être exécuté en parallèle avec la multiplication scalaire de Montgomery afin de calculer de façon concourante une partie de la multiplication scalaire. Nous présentons également deux formules pour le thirding de point dans une sous-famille de courbes $E(GF(3^m))$. Nous utilisons ces formules pour implémenter la multiplication scalaire à travers une approche de type third-and-add et une approche parallèle third-and-add et double-and-add ou triple-and-add. Nous fournissons également quelques résultats d'implantation sur un Intel Core i7 des deux stratégies proposées qui montrent une accélération de 5% -13% par rapport aux approches non parallélisées.

— G. Revy. Automated design of floating-point logarithm functions on integer processors. In *ARITH 23*, IEEE Symposium on Computer Arithmetic, Silicon Valley, Santa Clara, CA, United States, July 2016.

Résumé : De nos jours, la conception automatisée d'implantations efficaces de fonctions élémentaires (comme $\cos, \sin, \log, \exp, \ldots$) en arithmétique flottante et avec arrondi correct est un réel challenge. En effet, la diversité des architectures matérielles et des formats de données flottants rend ce processus d'implantation fastidieux. Cet article s'intéresse au cas particulier de la fonction $\log_b(x)$ sur processeurs entiers. Premièrement, il propose une réduction d'argument unifiée pour $\log_b(x)$, qui permet de réduire l'évaluation de ces fonctions à celle d'un seul polynôme bien choisi. Deuxièmement, il donne des conditions suffisantes sur les erreurs d'approximation et d'évaluation pour garantir l'arrondi correct de l'implantation. Et troisièmement, il montre comment automatiser le processus d'implantation de la fonction $\log_b(x)$ sur processeurs entiers, pour $b \in 2, exp(1), 10$. Finalement, nous montrons que cette approche automatisée permet d'accélérer la conception d'implantations efficaces de $\log_b(x)$, pour les formats de données standards.

9.2 HDR et thèses

Sur la période :
— 2 HDR soutenues
— 5 thèses soutenues
— 3 thèses en cours

Devenir des docteurs (soutenance sur la période) :
— 1 chercheur MathWorks (Cambridge, GB)
— 1 post-doctorant à l'Université de Liège (Institut Montefiore, Département d'Electricité Electronique & Informatique)
— 2 post-doctorants en France (LIP, DALI)
— 1 chercheur statutaire associé (DALI et rectorat de Montpellier)

9.3 Logiciels

CGPE (Code Generation for Polynomial Evaluation) est un outil logiciel qui permet de synthétiser du code rapide (optimisé pour une architecture cible) et certifié pour l'évaluation d'expressions mathématiques (polynômes univariés et bivariés, produits scalaires, sommes). Il permet la synthèse de codes pour les arithmétiques à virgule fixe et flottante, ou bien la description d'une architecture en VHDL. CGPE a notamment déjà été utilisé pour écrire automatiquement environ 50% du code de la bibliothèque FLIP, optimisée pour le ST231 (processeur entier VLIW 4 voies de ST Microelectronics).
Distribué sous licence CeCILL v-2 et accessible à http ://webdali.univ-perp.fr/logiciels.php

exBLAS est une bibliothèque C++/OpenCL de routines d'algèbre linéaire (BLAS) permettant de calculer de façon reproductible et précise sur les architectures multicœurs (GPU, Intel Xeon Phi).
6000 lignes de code accessibles à https ://exblas.lip6.fr/

FLIP (Floating-point Library for Integer Processor) est un outil logiciel pour la synthèse de codes certifiés pour l'évaluation de certains blocs de base d'algèbre linéaire en virgule fixe. Il permet en particulier d'écrire automatiquement du code pour la multiplication de matrices, ou bien l'inversion de matrices à base de décomposition de Cholesky. FPLA repose sur CGPE, qu'il utilise en backend.
Accessible à http ://webdali.univ-perp.fr/logiciels.php

FPLA (Fixed-Point Linear Algebra) est une bibliothèque C qui fournit un support logiciel pour l'arithmétique flottante simple précision (binary32) aux processeurs entiers. Elle propose notamment une implantation logicielle des 5 opérations de base, avec nombres dénormalisés et pour les 4 modes d'arrondi requis par le standard IEEE 754-2008. Cette bibliothèque cible particulièrement les processeurs VLIW et DSP. Elle a été validée sur les processeurs de la famille ST200 de ST Microelectronics.
Accessible à http ://webdali.univ-perp.fr/logiciels.php

FuzzyGPU est une bibliothèque C++/OpenCL d'opérateurs arithmétiques permettant de gérer les nombres flous symétriques.
2000 lignes de code accessible à https ://code.google.com/p/fuzzy-gpu/

GPUBurn est une bibliothèque C++/OpenCL/CUDA d'outils permettant de tester et localiser les erreurs intermittentes des GPU et de confiner le calcul aux seules unités saines.
1500 lignes de code accessibles à https ://code.google.com/p/gpuburn/

RARE-BLAS (Reproducible and Accurately Rounded BLAS) fournit une implémentation de l'interface BLAS, correctement arrondie pour le format binary64 de l'IEEE754. Elle exploite, de façon et optimisée et transparente pour l'utilisateur, les algorithmes de sommation récents les plus efficaces. Des calculs en précisions intermédiaires sont optimisés pour garantir la meilleure précision et la meilleure performance. Cette bibliothèque parallèle C/openMP/MPI fournit reproductibilité et précision sur les architectures multicœurs (CPU ou accélérateur Intel Xeon Phi).
Accessible à http ://webdali.univ-perp.fr/logiciels.php

10 Implication Formation/Recherche

— Coordination scientifique du mésocentre HPC@LR
— Co-organisation d'une série de 10 formations/an sur le HPC impliquant industriels et académiques pour le mésocentre HPC@LR
— Interventions dans les écoles thématiques du CNRS Archi (2013, 2015, 2017), écoles GIPSALAB (été 2013, hiver 2015), EJCIM (2013)
— Coordination et animations d'ateliers aux manifestations de médiation scientifique (village des sciences, ...)
— Conseil de l'Ecole Doctorale ED 305 (UPVD)

11 Implication dans les structures

— GDR Informatique Mathématique : comité de direction
— GDR Informatique Mathématique : responsabilité du groupe de travail Arith
— UPVD : direction du département Mathématiques-Informatique UPVD (2012-2014)
— UPVD : vice-présidence UPVD (VP Valorisation jusqu'en 2015)
— UPVD : comité de pilotage du Contrat Enseignant Pédagogie Innovante (CEPI)
— UPVD : mandats électifs aux CAC et CUFR, responsabilités de diplômes et présidences de jury

Publications 2013 – 2016

Articles dans des revues internationales

[ART.1] C. Negre et T. Plantard. "Efficient Regular Modular Exponentiation Using Multiplicative Half-Size Splitting". In : *Journal of Cryptographic Engineering* (2016). DOI : 10.1007/s13389-016-0134-5. URL : https://hal.archives-ouvertes.fr/hal-01185249.

[ART.2] M. Martel, M. A. Najahi et G. Revy. "Trade-offs of certified fixed-point code synthesis for linear algebra basic blocks". In : *Journal of Systems Architecture* (déc. 2016). DOI : 10.1016/j.sysarc.2016.11.010. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01279628.

[ART.3] M. Marin, D. Defour et F. Milano. "An efficient representation format for fuzzy intervals based on symmetric membership functions". In : *ACM Transactions on Mathematical Software* 43.3 (oct. 2016), 23 :1–23 :22. DOI : 10.1145/2939364. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01385459.

[ART.4] L. Thévenoux, P. Langlois et M. Martel. "Automatic source-to-source error compensation of floating-point programs : code synthesis to optimize accuracy and time". In : *Concurrency and Computation : Practice & Experience* (août 2016). DOI : 10.1002/cpe.3953. URL : https://hal.archives-ouvertes.fr/hal-01236919.

[ART.5] D. Defour et E. Petit. "A software scheduling solution to avoid corrupted units on GPUs". In : *Journal of Parallel and Distributed Computing* (fév. 2016), In Press. DOI : 10.1016/j.jpdc.2016.01.001. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01267742.

[ART.6] S. Collange, D. Defour, S. Graillat et R. Iakymchuk. "Numerical Reproducibility for the Parallel Reduction on Multi- and Many-Core Architectures". In : *Parallel Computing* 49 (nov. 2015), p. 83–97. DOI : 10.1016/j.parco.2015.09.001. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01206348.

[ART.7] C. Negre et J.-M. Robert. "New Parallel Approaches for Scalar Multiplication in Elliptic Curve over Fields of Small Characteristic". In : *IEEE Transactions on Computers* 64.10 (sept. 2015), p. 2875–2890. DOI : 10.1109/TC.2015.2389817. URL : https://hal.archives-ouvertes.fr/hal-00908463.

[ART.8] M. François, T. Grosges, D. Barchiesi et R. Erra. "Pseudo-random number generator based on mixing of three chaotic maps". In : *Communications in Nonlinear Science and Numerical Simulation* 19.4 (2014), p. 887–895. DOI : 10.1016/j.cnsns.2013.08.032. URL : https://hal.inria.fr/hal-00936657.

[ART.9] M. Cenk, A. Hasan et C. Negre. "Efficient Subquadratic Space Complexity Binary Polynomial Multipliers Based On Block Recombination". In : *IEEE Transactions on Computers* 63.9 (sept. 2014), p. 2273–2287. DOI : 10.1109/TC.2013.105. URL : https://hal.inria.fr/hal-00712090.

[ART.10] F. Jézéquel, P. Langlois et N. Revol. “First steps towards more numerical reproducibility”. In : *ESAIM : Proceedings*. ESAIM : Proceedings 45 (sept. 2014), p. 229–238. DOI : 10.1051/proc/201445023. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-00872562.

[ART.11] M. François, D. Defour et C. Negre. “A Fast Chaos-Based Pseudo-Random Bit Generator Using Binary64 Floating-Point Arithmetic”. In : *Informatica* 38.2 (juil. 2014), p. 115–124. URL : https://hal.archives-ouvertes.fr/hal-01024689.

[ART.12] C. Negre. “Efficient Binary Polynomial Multiplication Based on Optimized Karatsuba Reconstruction”. In : *Journal of Cryptographic Engineering* 4.2 (juil. 2014), p. 91–106. DOI : 10.1007/s13389-013-0066-2. URL : https://hal.inria.fr/hal-00724778.

[ART.13] M. Cenk, C. Negre et A. Hasan. “Improved Three-Way Split Formulas for Binary Polynomial and Toeplitz Matrix Vector Products”. In : *IEEE Transactions on Computers* 62.7 (juil. 2013), p. 1345–1361. URL : https://hal.archives-ouvertes.fr/hal-00839945.

[ART.14] A. Hasan et C. Negre. “Multiway Splitting Method for Toeplitz Matrix Vector Product”. In : *IEEE Transactions on Computers* 62.7 (juil. 2013), p. 1467–1471. DOI : 10.1109/TC.2012.95. URL : https://hal.archives-ouvertes.fr/hal-00839952.

[ART.15] J. Adikari, A. Barsoum, A. Hasan, A. H. Namin et C. Negre. “Improved Area-Time Trade-offs for Field Multiplication using Optimal Normal Bases”. In : *IEEE Transactions on Computers* 62.1 (jan. 2013), p. 193–199. DOI : 10.1109/TC.2011.198. URL : https://hal.archives-ouvertes.fr/hal-00813784.

Conférences avec actes - audience internationale

[CACT.1] R. Nheili, P. Langlois et C. Denis. “First improvements toward a reproducible Telemac-2D”. In : *XXIIIrd TELEMAC-MASCARET User Conference*. Paris, France, oct. 2016. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01371152.

[CACT.2] C. Chohra, P. Langlois et D. Parello. “Parallel experiments with RARE-BLAS”. In : *SYNASC : Symbolic and Numeric Algorithms for Scientific Computing*. Timisoara, Romania, sept. 2016. URL : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01349698.

[CACT.3] C. Chohra, P. Langlois et D. Parello. “Reproducible, Accurately Rounded and Efficient BLAS”. In : *REPPAR : Reproducibility in Parallel Computing*. Grenoble, France, août 2016. URL : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01280324.

[CACT.4] P. Langlois, R. Nheili et C. Denis. “Recovering numerical reproducibility in hydrodynamic simulations”. In : *ARITH : Computer Arithmetic*. Silicon Valley, Santa Clara, CA, United States, juil. 2016. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01274671.

[CACT.5] A. Lesavourey, C. Negre et T. Plantard. “Efficient Randomized Regular Modular Exponentiation using Combined Montgomery and Barrett Multiplications”. In : *SECRYPT : Security and Cryptography*. Lisbon, Portugal, juil. 2016. URL : https://hal.archives-ouvertes.fr/hal-01330898.

[CACT.6] T. Plantard et J.-M. Robert. "Enhanced Digital Signature using RNS Digit Exponent Representation". In : *International Workshop on the Arithmetic of Finite Fields, WAIFI 2016*. lncs. Department of Mathematics of Ghent University. Gand, Belgium : Springer, juil. 2016. URL : https://hal.archives-ouvertes.fr/hal-01337561.

[CACT.7] G. Revy. "Automated design of floating-point logarithm functions on integer processors". In : *ARITH 23*. Silicon Valley, Santa Clara, CA, United States, juil. 2016. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01276677.

[CACT.8] C. Chohra, P. Langlois et D. Parello. "Efficiency of Reproducible Level 1 BLAS". In : t. 9553. Scientific Computing, Computer Arithmetic, and Validated Numerics. 16th International Symposium, SCAN 2014, Würzburg, Germany. September 21-26, 2014. Revised Selected Papers. springer, avr. 2016. DOI : 10.1007/978-3-319-31769-4_8. URL : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01101723.

[CACT.9] R. Iakymchuk, D. Defour, S. Collange et S. Graillat. "Reproducible and Accurate Algorithms for Numerical Linear Algebra". In : *PP : Parallel Processing for Scientific Computing*. Paris, France : SIAM, avr. 2016. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01268048.

[CACT.10] B. Goossens, D. Parello, K. Porada et D. Rahmoune. "Parallel Locality and Parallelization Quality". In : *PMAM : Programming Models and Applications for Multicores and Manycores*. Barcelona, Spain, mar. 2016. DOI : 10.1145/2883404.2883410. URL : https://hal.archives-ouvertes.fr/hal-01252007.

[CACT.11] L. Thévenoux, P. Langlois et M. Martel. "Automatic Source-to-Source Error Compensation of Floating-Point Programs". In : *CSE : Computational Science and Engineering*. Porto, Portugal, oct. 2015. DOI : 10.1109/CSE.2015.11. URL : https://hal.archives-ouvertes.fr/hal-01158399.

[CACT.12] D. Defour. "Measuring predictability of Nvidia's GPU warp and block schedulers : Application to the summation problem". In : *IEEE 9th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC-15)*. Turin, Italy, sept. 2015, p. 17–24. DOI : 10.1109/MCSoC.2015.9. URL : https://hal.archives-ouvertes.fr/hal-01267747.

[CACT.13] D. Defour et S. Collange. "Reproducible floating-point atomic addition in data-parallel environment". In : *ACSIS : Annals of Computer Science and Information Systems*. T. 5. Lodz, Poland, sept. 2015, p. 721–728. DOI : 10.15439/2015F86. URL : https://hal.archives-ouvertes.fr/hal-01267755.

[CACT.14] B. Goossens, D. Parello, K. Porada et D. Rahmoune. "Toward a Core Design to Distribute an Execution on a Many-Core Processor". In : *PaCT : Parallel Computing Technologies*. Sous la dir. de V. Malyshkin. T. LNCS. Parallel Computing Technologies 9251. Petrozavodsk, Russia : Springer International Publishing, août 2015, p. 390–404. DOI : 10.1007/978-3-319-21909-7_38. URL : https://hal.archives-ouvertes.fr/hal-01152664.

[CACT.15] P. Langlois, R. Nheili et C. Denis. “Numerical Reproducibility : Feasibility Issues”. In : *NTMS : New Technologies, Mobility and Security*. Sous la dir. de M. Badra, A. Boukerche et P. Urien. Paris, France, juil. 2015. doi : 10.1109/NTMS.2015.7266509. url : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01141852.

[CACT.16] H. de Lassus Saint-Geniès, D. Defour et G. Revy. “Range Reduction Based on Pythagorean Triples for Trigonometric Function Evaluation”. In : *ASAP : Application-Specific Systems, Architectures and Processors*. Toronto, Canada : IEEE, juil. 2015, p. 74–81. doi : 10.1109/ASAP.2015.7245712. url : https://hal.archives-ouvertes.fr/hal-01134232.

[CACT.17] C. Negre et J.-M. Robert. “Parallel Approaches for Efficient Scalar Multiplication over Elliptic Curve”. In : *SECRYPT : International Conference on Security and Cryptography*. Colmar, France : SciTePress, juil. 2015, p. 202–209. doi : 10.5220/0005512502020209. url : https://hal.archives-ouvertes.fr/hal-01206530.

[CACT.18] R. Nheili, P. Langlois et C. Denis. “Numerical Reproducibility in open TELEMAC : A Case Study within the Tomawac Library”. In : *2nd International Workshop on High Performance Computing Simulation in Energy/Transport Domains (HPCSET 2015), ISC High Performance 2015 Conference*. Frankfurt, Germany, juil. 2015. url : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01101715.

[CACT.19] H. de Lassus Saint-Geniès, D. Defour et G. Revy. “Réduction d’argument basée sur les triplets pythagoriciens pour l’évaluation de fonctions trigonométriques”. In : *ComPAS : Conférence en Parallélisme, Architecture et Système*. Lille, France, juin 2015. url : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01136772.

[CACT.20] C. Negre et G. Perin. “Trade-off Approaches for Leak Resistant Modular Arithmetic in RNS”. In : *ACISP : Australasian Conference on Information Security and Privacy*. Sous la dir. d’E. Foo et D. Stebila. T. LNCS. Information Security and Privacy 9144. Brisbane, Australia : Springer, juin 2015, p. 107–124. doi : 10.1007/978-3-319-19962-7_7. url : https://hal.archives-ouvertes.fr/hal-01143367.

[CACT.21] C. Negre, T. Plantard et J.-M. Robert. “Efficient Modular Exponentiation Based on Multiple Multiplications by a Common Operand”. In : *ARITH : Computer Arithmetic*. INRIA. Lyon, France, juin 2015, p. 144–151. doi : 10.1109/ARITH.2015.24. url : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01142327.

[CACT.22] R. Iakymchuk, D. Defour, S. Collange et S. Graillat. “Reproducible Triangular Solvers for High-Performance Computing”. In : *ITNG : Information Technology - New Generations*. Las Vegas, NV, United States, avr. 2015, p. 353–358. doi : 10.1109/ITNG.2015.63. url : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01206371.

[CACT.23] C. Negre et J.-M. Robert. “Recent Advances in Parallel Implementations of Scalar Multiplication over Binary Elliptic Curves”. In : *RAIM : Rencontres Arithmétiques de l’Informatique Mathématique*. A.Tisserand and D. Menard and S. Duquesne and S. Collange and N. SaintPierre. Rennes, France, avr. 2015. url : https://hal.archives-ouvertes.fr/hal-01141628.

[CACT.24] J.-M. Robert. “Software Implementation of Parallelized ECSM over Binary and Prime Fields”. In : *Inscrypt : Information Security and Cryptology*. T. LNCS. 8957. Beijing, China : Springer, déc. 2014, p. 445–462. doi : 10.1007/978-3-319-16745-9_24. url : https://hal.archives-ouvertes.fr/hal-00998277.

[CACT.25] M. Martel, M. A. Najahi et G. Revy. “Toward the synthesis of fixed-point code for matrix inversion based on Cholesky decomposition”. In : *DASIP : Design and Architectures for Signal and Image Processing*. Madrid, Spain : IEEE, oct. 2014, p. 1–8. doi : 10.1109/DASIP.2014.7115609. url : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01212806.

[CACT.26] C. Chohra, P. Langlois et D. Parello. “Level 1 Parallel RTN-BLAS : Implementation and Efficiency Analysis”. In : *SCAN : Scientific Computing, Computer Arithmetic and Validated Numerics*. Wurzburg, Germany, sept. 2014. url : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01095172.

[CACT.27] C. Mouilleron, M. A. Najahi et G. Revy. “Automated Synthesis of Target-Dependent Programs for Polynomial Evaluation in Fixed-Point Arithmetic”. In : *SYNASC : Symposium on Symbolic and Numeric Algorithms for Scientific Computing*. Timisoara, Romania, sept. 2014, p. 141–148. doi : 10.1109/SYNASC.2014.27. url : https://hal-lirmm.ccsd.cnrs.fr/lirmm-00814338.

[CACT.28] S. Collange, D. Defour, S. Graillat et R. Iakymchuk. “A Reproducible Accurate Summation Algorithm for High-Performance Computing”. In : *EX : Exascale Applied Mathematics Challenges and Opportunities*. Chicago, United States, juil. 2014. url : https://hal.archives-ouvertes.fr/hal-01267825.

[CACT.29] M. Marin, D. Defour et F. Milano. “Power Flow Analysis under Uncertainty using Symmetric Fuzzy Arithmetic”. In : *PES General Meeting 2014 | Conference & Exposition*. National Harbor, MD, United States : IEEE, juil. 2014, p. 1–5. doi : 10.1109/PESGM.2014.6939274. url : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01206373.

[CACT.30] D. Defour. “Impact des schedulers sur la prédictibilité dans les GPU”. In : *ComPAS : Conférence en Parallélisme, Architecture et Système*. Sous la dir. de P. Felber, L. Philippe, E. Riviere et A. Tisserand. Neuchâtel, Switzerland, avr. 2014. url : https://hal.archives-ouvertes.fr/hal-00951916.

[CACT.31] M. François, D. Defour et P. Berthomé. “A Pseudo-Random Bit Generator Based on Three Chaotic Logistic Maps and IEEE 754-2008 Floating-Point Arithmetic”. In : *Theory and Applications of Models of Computation*. Sous la dir. de T. Gopal, A. L. A. B. Cooper et M. Agrawal. LNCS 8402. Chennai, India : Springer, avr. 2014, p. 229–247. doi : 10.1007/978-3-319-06089-7_16. url : https://hal.archives-ouvertes.fr/hal-00985357.

[CACT.32] K. Porada, D. Parello et B. Goossens. “Analyse et réduction du chemin critique dans l’exécution d’une application”. In : *ComPAS : Conférence en Parallélisme, Architecture et Système*. Neuchâtel, Switzerland, avr. 2014. url : https://hal.inria.fr/hal-01158433.

[CACT.33] M. Marin et D. Defour. “FuzzyGPU : a fuzzy arithmetic library for GPU”. In : *PDP : Parallel, Distributed and Network-Based Processing*. Torino, Italy : IEEE, fév. 2014, p. 624–631. DOI : 10.1109/PDP.2014.16. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01206375.

[CACT.34] M. Martel, M. A. Najahi et G. Revy. “Code Size and Accuracy-Aware Synthesis of Fixed-Point Programs for Matrix Multiplication”. In : *PECCS : Pervasive and Embedded Computing and Communication Systems*. Lisbonne, Portugal, jan. 2014. DOI : 10.5220/0004884802040214. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-00860383.

[CACT.35] E. Petit et D. Defour. “GPUburn : A System to Test and Mitigate GPU Hardware Failures”. In : *SAMOS : Embedded Computer Systems : Architectures, Modeling, and Simulation*. Samos, Greece, juil. 2013, p. 263–270. DOI : 10.1109/SAMOS.2013.6621133. URL : https://hal.archives-ouvertes.fr/hal-00827588.

[CACT.36] D. Defour et M. Marin. “Regularity versus Load-Balancing on GPU for treefix computations”. In : *ICCS : International Conference on Computational Science*. T. 18. Barcelone, Spain, juin 2013, p. 309–318. URL : https://hal.archives-ouvertes.fr/hal-00768293.

[CACT.37] A. Ioualalen et M. Martel. “Synthesizing Accurate Floating-Point Formulas”. In : *ASAP : Application-Specific Systems, Architectures and Processors*. Washington, DC, United States : IEEE, juin 2013, p. 113–116. DOI : 10.1109/ASAP.2013.6567563. URL : https://hal.archives-ouvertes.fr/hal-00835736.

[CACT.38] C. Negre et J.-M. Robert. “Impact of Optimized Operations AB,AC and AB+CD in Scalar Multiplication over Binary Elliptic Curve”. In : *AFRICACRYPT : Cryptology in Africa*. T. LNCS. Progress in Cryptology – AFRICACRYPT 2014 8469. Cairo, Egypt, juin 2013, p. 13–30. DOI : 10.1007/978-3-642-38553-7_16. URL : https://hal.inria.fr/hal-00724785.

[CACT.39] P. Langlois, B. Goossens et D. Parello. “Towards a Reliable Performance Evaluation of Accurate Summation Algorithms”. In : *SCE : Computational Science and Engineering*. SIAM. Boston, Ma, United States, fév. 2013. URL : https://hal.archives-ouvertes.fr/hal-01233879.

Autres conférences

[COMN.1] R. S. Iakymchuk, S. S. Graillat, D. Defour et E. S. Quintana-Ortí. “Hierarchical Approach for Deriving a Reproducible LU factorization on GPUs”. In : *The Numerical Reproducibility at Exascale (NRE16) workshop held as part of the Supercomputing Conference (SC16)*. Salt Lake City, UT, United States, nov. 2016. URL : https://hal.archives-ouvertes.fr/hal-01382645.

[COMN.2] H. de Lassus Saint-Geniès et G. Revy. “Performances de schémas d’évaluation polynomiale sur architectures vectorielles”. In : *ComPAS : Conférence en Parallélisme, Architecture et Système*. Laboratoire des Sciences et Techniques de l’Information, de la Communication et de la Connaissance (Lab-STICC). Lorient, France, juil. 2016. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01324740.

[COMN.3] R. Iakymchuk, S. Collange, D. Defour et S. Graillat. "ExBLAS : Reproducible and Accurate BLAS Library". In : *NRE : Numerical Reproducibility at Exascale*. Austin, TX, United States, nov. 2015. URL : https://hal.archives-ouvertes.fr/hal-01202396.

[COMN.4] R. Iakymchuk, S. Collange, D. Defour et S. Graillat. "Reproducibility and Accuracy for High-Performance Computing". In : *RAIM : Rencontres Arithmétiques de l'Informatique Mathématique*. Rennes, France, avr. 2015. URL : https://hal.archives-ouvertes.fr/hal-01140531.

[COMN.5] M. Marin, D. Defour et F. Milano. "An efficient midpoint-radius implementation to handle symmetric fuzzy intervals". In : *RAIM : Rencontres Arithmétiques de l'Informatique Mathématique*. Rennes, France, avr. 2015. URL : https://hal.archives-ouvertes.fr/hal-01140504.

[COMN.6] M. A. Najahi. "Synthesis of certified programs in fixed-point arithmetic, and its application to linear algebra basic blocks". In : *RAIM : Rencontres Arithmétiques de l'Informatique Mathématique*. Rennes, France, avr. 2015. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01277374.

[COMN.7] R. Nheili, P. Langlois et C. Denis. "Solutions to ensure the reproducibility of the digital simulation of the effect of waves on the coast". In : *RAIM : Rencontres Arithmétiques de l'Informatique Mathématique*. Rennes, France, avr. 2015. URL : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01179997.

[COMN.8] J.-M. Robert. "Algorithmes Parallèles de Multiplication Scalaire Optimisée sur Courbes Elliptiques Binaires". In : *C2 : Journées Codage et Cryptographie*. GT-C2. Les Sept-Laux, France, mar. 2014. URL : http://hal-lirmm.ccsd.cnrs.fr/lirmm-01121960.

[COMN.9] D. Defour et E. Petit. "Températures, erreurs matérielles et GPU". In : *ComPAS : Conférence en Parallélisme, Architecture et Système*. Grenoble, France, jan. 2013, p. 1–11. URL : https://hal.archives-ouvertes.fr/hal-00785386.

[COMN.10] D. Parello, B. Goossens et P. Langlois. "Améliorer l'analyse de la performance des algorithmes numériques". In : *ComPAS : Conférence en Parallélisme, Architecture et Système*. Grenoble, France, jan. 2013. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-00762550.

[COMN.11] D. Parello, P. Langlois et B. Goossens. "Sur la reproductibilité des mesures des performances d'algorithmes numériques avec PerPI". In : *ComPAS : Conférence en Parallélisme, Architecture et Système*. Grenoble, France, jan. 2013. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-00762024.

Conférences invitées

[INV.1] R. Iakymchuk, D. Defour, S. Collange et S. Graillat. "Reproducible and Accurate Algorithms for Numerical Linear Algebra". In : *PP : Parallel Processing for Scientific Computing*. Paris, France : SIAM, avr. 2016. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01268048.

[INV.2] P. Langlois, C. Chohra et R. Nheili. “Cas d’études de calculs parallèles numériquement reproductibles”. In : *Retour d’expéRiences sur la Recherche Reproductible*. MISC/CaSciModOT. Orléans, France, déc. 2015. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-01240737.

[INV.3] C. Negre et J.-M. Robert. “Recent Advances in Parallel Implementations of Scalar Multiplication over Binary Elliptic Curves”. In : *RAIM : Rencontres Arithmétiques de l’Informatique Mathématique*. A.Tisserand and D. Menard and S. Duquesne and S. Collange and N. SaintPierre. Rennes, France, avr. 2015. URL : https://hal.archives-ouvertes.fr/hal-01141628.

Direction d’ouvrages et de proceedings

[DOUV.1] P. Langlois. *Informatique Mathématique : une photographie en 2013*. Sous la dir. de P. Langlois. Etudes. Presses Universitaires de Perpignan, avr. 2013, p. 283. URL : https://hal-lirmm.ccsd.cnrs.fr/lirmm-00835506.

Chapitres d’ouvrages

[COUV.1] D. Defour et M. Marin. “Simulation temps réel de réseaux électriques à l’aide des architectures multicœurs”. In : *UPVD Magazine Hors-Série recherche*. 3. 2014, p. 42–44. URL : https://hal.archives-ouvertes.fr/hal-01267852.

[COUV.2] D. Defour et M. Marin. “Optimiser la représentation des flottants”. In : *HPC Today*. T. 4. Juin 2013, p. 65–70. URL : https://hal.archives-ouvertes.fr/hal-01267953.

Liste des thèses et HDR 2013 – 2016

Thèses soutenues

— **Laurent Thévenoux**. Soutenance juillet 2014.
Synthèse de code avec compromis entre performance et précision en arithmétique flottante IEEE 754.
Encadrement : Ph. Langlois, M. Martel
septembre 2010 → juillet 2014.
— Financement 1 sur programme chercheur d'avenir Région (36 mois)
— Financement 2 sur emploi ATER (11 mois)

— **Amine Najahi**. Soutenance décembre 2014.
Synthesis of certified programs in fixed-point arithmetic, and its application to linear algebra basic blocks.
Encadrement : M. Martel, G. Revy.
novembre 2011 → décembre 2014.
— Financement 1 par crédits ANR (34 mois)
— Financement 2 sur emploi ATER (4 mois)

— **Manuel Marin**. Soutenance décembre 2015.
GPU-enhanced power flow analysis.
Encadrement : D. Defour, F. Milano
septembre 2012 → décembre 2015.
— Financement par Ecole Doctorale ED305 (36 mois)

— **Jean-Marc Robert**. Soutenance décembre 2015.
Contrer l'attaque Simple Power Analysis efficacement dans les applications de la cryptographie asymétrique, algorithmes et implantations.
Encadrement : B. Goossens, Ch. Negre.
septembre 2012 → décembre 2015.
— Financement par crédits ANR (40 mois)

— **Rafife Nheili**. Soutenance décembre 2016.
How to improve the numerical reproducibility of hydrodynamics simulations : analysis and solutions for one open-source HPC software.
Encadrement : Ph. Langlois, Ch. Denis (EDF R&D)
novembre 2013 → décembre 2016.
— Financement 1 sur programme Erasmus Peace 2 (30 mois)
— Financement 2 sur contrat de recherche avec EDF R&D (6 mois)

Thèses en cours

— **Chemseddine Chohra**. $4^{ème}$ année. Soutenance le 10 mars 2017.
Towards Reproducible, Accurately Rounded and Efficient BLAS.
Encadrement : Ph. Langlois, D. Parello.
septembre 2013 → mars 2017.
— Financement sur programme d'excellence du gouvernement Algérien (39 mois)

— **Kathy Porada**. $3^{ème}$ année.
A manycore processor to automatically parallelize a run and a deterministic parallel programming model.
Encadrement : B. Goossens, G. Sassatelli.
septembre 2014 →
— Financement par crédits européens (36 mois)

— **Hugues de Lassus Saint-Geniès**. $3^{ème}$ année.
Génération de codes hautes performances sous contraintes architecturales appliquée aux fonctions mathématiques.
Encadrement : D. Defour, G. Revy.
octobre 2014 →
— Financement par crédits ANR (36 mois)

HDR soutenues

— **David Defour.** Soutenance en octobre 2014.
Contribution au calcul sur GPU : considérations arithmétiques et architecturales.

— **Christophe Negre.** Soutenance en juin 2016.
Multiplication in finite fields and elliptic curves.

Projets 2013–2016

Valorisation

Actility (2013-2014) Montant : 14000 €. Convention UPVD, DRV (451REC03)

3E (2015-2016) Montant : 14000 €. Convention UPVD, DRV (451REC04)

EDF R&D (2016-2017) Montant : 19400 €. Convention CNRS, DR LR (EDF-LIRMM CT 133129)

Collaboration

ANR INS DEFIS (2011-2015) http ://defis.lip6.fr/

Partenaires : IRISA/Lannion, LIP6/UPMC Paris, LIRMM/Perpignan, CEA LIST/Saclay, THALES/Paris et Inpixal/Rennes.

Dotation : 994498 €.

Pour des raisons de consommation d'énergie, de surface et/ou de coût de conception, certaines architectures ne proposent pas de support matériel à l'arithmétique flottante. Une alternative consiste alors à utiliser l'arithmétique virgule fixe, ce qui rend le développement d'applications numériques coûteux en temps. L'objectif du projet ANR DEFIS est de proposer un flot automatisé de génération de codes en virgule fixe, travaillant à partir d'une application existante ou de briques de base (évaluation polynomiale, multiplication/inversion de matrices, ...). Ce projet a donné lieu au développement de nombreux outils, qui ont été validés en partie sur les applications industrielles de THALES et Inpixal.

ANR INS MetaLibm (2014-2017) http ://www.metalibm.org/ANRMetaLibm/

Partenaires : Inria/INSA Lyon, LIP/ENS Lyon, LIP6/UPMC Paris, LIRMM/Perpignan et CERN/Genève.

Dotation : 622782 €.

Le développement d'applications numériques reposent très souvent sur l'utilisation de bibliothèques mathématiques. L'écriture optimisée de ces bibliothèques requiert de connaître parfaitement l'architecture sur laquelle elle est censé être utilisée, à savoir son jeu d'instructions, ses unités de calculs, ses caractéristiques arithmétiques et de mémoire, ... L'objectif du projet ANR MetaLibm est de proposer des outils automatisés pour la génération de codes flottants pour l'évaluation de fonctions mathématiques (fonctions logarithme, exponentiel, trigonométriques, ...) et de filtres, optimisés pour une architecture à caractéristiques données (support vectoriel et/ou scalaire, arithmétique binary32/64, ...).

ANR PAVOIS (2012-2016) http ://pavois.irisa.fr/

Partenaires : DALI/LIRMM, IRISA

Dotation : 348868 €

L'ANR Pavois fait intervenir deux pôles : DALI/LIRMM et l'IRISA (Lannion). Elle a pour but d'améliorer la sécurité des implantations embarquées. Le pôle DALI/LIRMM, et plus particulièrement la thèse de J.-M. Robert a pour but de proposer de nouvelles approches algorithmiques pour contrer ces attaques matérielles, le point de vue matériel étant étudié plus profondément à Lannion. Nous avons exploré des approches régulières, parallèles et séquentielles, protégeant les implantations contre la Simple Power Analysis. Nous avons aussi proposé des contre-mesures contre la DPA basées sur la randomisation des calculs.

PEPS QUARENUM (2013) https ://www.lri.fr/ baboulin/quarenum.html

Partenaires : LRI, LIP6, LIP/ENS Lyon, LIRMM, EDF R&D.

Dotation : 5000 €.

Le projet QUARENUM (QUAlity and REproducibility in NUMerical applications on the road to Exascale) vise à concevoir et implémenter des algorithmes efficaces pour la validation et la reproductibilité numériques en calcul haute-performance (HPC). Ce projet s'intéresse plus particulièrement aux méthodes d'analyse de la sensibilité des applications HPC aux erreurs (e.g., simulation de la propagation des erreur par arithmétiques stochastique ou d'intervalles, estimation de nombre de conditionnement et d'erreur inverse). Ces aspects et l'objectif de reproductibilité numérique sont étudié dans le contexte d'architectures massivement parallèles et hétérogènes.

Ce PEPS a permis la préparation des projets REQUIN et GRAAF soumis à l'ANR en 2014, 2015 et 2016 mais non retenus.