Bilan de l'activité de recherche et des résultats obtenus par l'équipe de recherche en Informatique

DALI : Digits, Architectures et Logiciels Informatiques

Laboratoire ELIAUS, UPVD.

Partie 1 : Bilan scientifique
Période 2005–2009

http://webdali.univ-perp.fr

19 mai 2009

Table des matières

1 Contexte général et motivation

DALI est l'équipe de recherche en informatique de l'UPVD. Créée *ex nihilo* en 2003, elle a d'abord été soutenue par une ACI Jeune Chercheur (ACI JC9276, 2003-2006). En 2007-2010, elle constitue une des trois équipes du laboratoire ELIAUS (EA 3679).

Pour 2011-2014, DALI propose de devenir une nouvelle équipe-projet du LIRMM (UM2, CNRS) dans le cadre d'une structuration à définir entre les trois tutelles UPVD, UM2 et CNRS.

Cet projet répond à des évolutions structurelles importantes tant au niveau local que régional et national.

- Les deux autres équipes d'ELIAUS, à dominante électronique et automatique, intégreront l'UPR CNRS PROMES (Procédés, Matériaux et Énergie Solaire) à partir de 2011.
- La masse critique actuelle de l'équipe DALI ne permet pas d'espérer une reconnaissance par le MESR comme équipe d'accueil de l'UPVD.
- Le LIRMM est l'entité de recherche régionale du domaine ST2I qui regroupe la très grande majorité des chercheurs et enseignants-chercheurs en informatique.

La suite de rapport présente le bilan scientifique de l'équipe DALI, en vue de son intégration comme nouvelle équipe-projet du LIRMM. Par conséquent, les activités d'un professeur recruté en 2007, actuellement rattaché à DALI et dont le projet est d'intégrer l'UPR CNRS PROMES (Procédés, Matériaux et Énergie Solaire) à partir de 2011, ne sont pas considérées dans ce document.

Composition de l'équipe. L'équipe DALI est composée de 8 emplois permanents d'enseignant-chercheur de 27ème section : 2 PR, 5 MCF (dont 1 HDR) et 1 ATER recherche récurrent (dotation Fillon 2004). Le tableau suivant synthétise le développement de l'équipe (hors ATER et doctorants) depuis sa création en 2003.

Année	Chercheur	Âge de recrutement	Origine
2003	B. Goossens : PR à l'UFR SEE	47	LIAFA, U. Paris 7
2003	Ph. Langlois : PR à l'IUT	40	IUT Perpignan
2004	D. Defour : MCF	27	LIP, ENS Lyon
2005	D. Parello : MCF	28	LRI, U. Orsay
2006	Ch. Nègre : MCF	29	LIRMM, U. Montpellier 2
2007	M. Martel : MCF HDR	34	LIST, CEA Saclay
2009	X : MCF		

Politique scientifique. Dès son origine, nous avons privilégié le développement d'une équipe de recherche avec un positionnement scientifique resserré autour de l'expertise des professeurs. L'équipe a systématiquement appliqué ce choix lors des recrutements — et s'est adaptée pour satisfaire les besoins d'enseignement d'une petite université pluridisciplinaire. Nous incitons au dynamisme et à la reconnaissances des actions scientifiques de l'équipe, à la mobilité (régionale, nationale, internationale) de ses membres et en particulier des plus jeunes d'entre eux ; nous sommes attentifs à la qualité de l'encadrement doctoral et soucieux de la dimension humaine de l'équipe. DALI affiche ainsi une forte attractivité de jeunes chercheurs de qualité sur la période concernée. L'implication et la reconnaissance de l'équipe dans les réseaux nationaux a contribué au succès de la mise en oeuvre de cette politique.

2 Une unité thématique : qualité numérique et haute performance des calculs

Une des forces de l'équipe de recherche DALI est l'unité thématique de ses travaux de recherche qui visent à **améliorer la qualité numérique et la haute performance des calculs**.

Dans cet objectif, DALI permet l'interaction, rare en France au sein d'une même équipe, d'experts en **architecture et micro-architecture, simulation et compilation et arithmétique des ordinateurs**. Les actions de recherche développées pendant la période 2005-2009 concernent à la fois le matériel (processeurs généralistes, architectures émergentes), le logiciel (arithmétique et précision), les outils de simulation ou de certification automatique, et les applications (algorithmique numérique, cryptographie, systèmes embarqués critiques, calcul formel, théorie du contrôle).

Objectif : améliorer la performance des calculs. L'amélioration de la performance des calculs est étroitement liée aux améliorations apportées aux micro-architectures. L'évolution des micro-architectures est guidée par l'évolution technologique et en particulier par l'augmentation du nombre de transistors et par leur miniaturisation. Les principales contraintes rencontrées, comme les problèmes de dissipation thermique ou la limite physique de miniaturisation des transistors, exigent des micro-architectures une exploitation des transistors toujours plus efficace. L'exploitation efficace du nombre croissant de transistors peut être réalisée suivant plusieurs directions : l'élargissement des chemins (micro-architecture vectorielle), l'augmentation de la hiérarchie mémoire (caches), la **multiplication des cœurs** (parallélisme de tâches), l'augmentation du **parallélisme d'instructions**.

Objectif : améliorer la qualité numérique. L'arithmétique des ordinateurs consiste à définir, prouver et implanter la meilleure adéquation entre, d'une part la représentation des nombres et les arithmétiques associées, et d'autre part, les applications. Un exemple classique est l'étude des **opérateurs arithmétiques pour la cryptographie**[1]. La qualité numérique des applications de calcul scientifique ou la sûreté de 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 numérique des calculs et des résultats**. Certaines applications, en calcul scientifique en particulier, nécessitent d'améliorer la qualité numérique des applications sans pour autant sacrifier la rapidité de l'exécution. Ainsi se rejoignent amélioration de la performance et de la qualité numérique.

Cinq actions de recherche qui profitent des compétences de l'équipe. Les travaux développés sur la période 2005-2009 sont organisés autour de 5 actions de recherche qui reprennent certains points précédemment identifiés.
- Action 1. Augmenter le degré superscalaire des processeurs
- Action 2. Exploiter les architectures émergentes haute-performance : GPGPU-Manycœur
- Action 3. Nouveaux algorithmes précis, validés et rapides
- Action 4. Certification et applications
- Action 5. Opérateurs arithmétiques pour la cryptographie

La figure 1 synthétise le positionnement de ces différentes actions en vue de l'objectif général de nos recherches ainsi que les interactions des principaux domaines de compétences de l'équipe.

Nous proposons maintenant un bilan très synthétique de chacune de ces actions.

[1] Cet axe de recherche est aussi développé au sein de l'équipe-projet Arith du LIRMM.

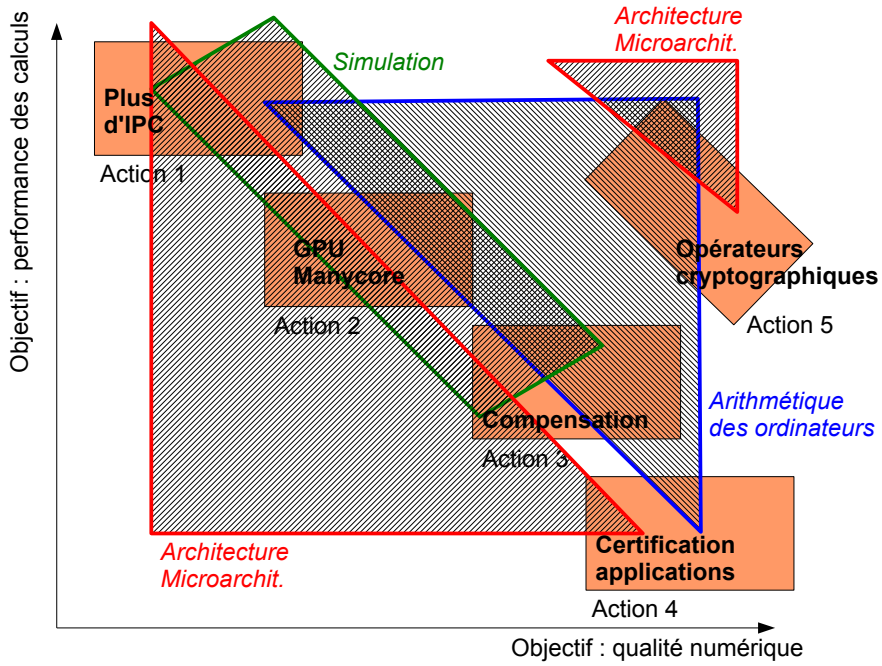

FIG. 1 – *Objectifs, actions et interactions au sein de DALI.*

2.1 Action 1. Augmenter le degré superscalaire des processeurs

Contexte et originalité de l'approche. La tendance actuelle est de consacrer les transistors supplémentaires du composant à la multiplication des cœurs et tirer parti du parallélisme de tâche plutôt que du parallélisme d'instruction.

Notre avis est que d'une part la multiplication des cœurs a ses limites qui ne sont sans doute pas loin d'être atteintes. D'autre part, le parallélisme d'instruction est loin d'être exploité efficacement. Le degré de parallélisme des codes entiers varie de 20 à 60 instructions exécutables par cycle et celui des codes flottants varie de 75 à 150 instructions exécutables par cycle alors que les processeurs actuels exécutent avec peine 2 instructions par cycle. Le potentiel est là, en majeure partie inexploité. Enfin, tirer avantage du parallélisme d'instruction ne se fait pas forcément au détriment du parallélisme de tâche (l'un empiète sur l'autre si l'un prive l'autre d'une partie des transistors).

Résultats obtenus. Pour mesurer l'efficacité des solutions proposées [72], il est nécessaire de disposer d'un outil de simulation souple et adaptable, représentatif aussi bien de processeurs génériques que de processeurs réels — pour se comparer à l'état de l'art et à l'état du marché. Le simulateur UNISIM[ACG+07][2] , a été adapté par notre équipe à cette fin. L'équipe DALI a dérivé un simulateur de processeur générique multi-cœur en s'appuyant sur une technique innovante de vectorisation des modules [59, 81], simplifiant la duplication des unités du processeur (opérateurs, cœurs) et accélérant la vitesse de simulation.

Travaux en cours. Avec cet outil, nous étudions différentes politiques d'ordonnancement du lancement des instructions. Notre but est de dégager des indications pour calibrer le matériel de façon à

[2]UNISIM est une plate-forme de simulation fédérant de nombreux instituts : INRIA Scalay, CEA List, Princeton University, Universitat Politècnica de Catalunya, Barcelona Supercomputing Center, Ghent University, Brigham Young University, Université de Perpignan, ARM, ST Microelectronics. http ://`www.unisim.org`.

[ACG+07] David August, Jonathan Chang, Sylvain Girbal, Daniel Gracia-Perez, Gilles Mouchard, David A. Penry, Olivier Temam, and Neil Vachharajani. Unisim: An open simulation environment and library for complex architecture design and collaborative development. *IEEE Comput. Archit. Lett.*, 6(2):45–48, 2007.

obtenir un ordonnancement remplissant mieux le pipeline de chaque cœur.

2.2 Action 2. Exploiter les architectures émergentes haute-performance : GPGPU-Manycœur

Contexte et originalité de l'approche. Les nouvelles architectures composées de plusieurs dizaines ou centaines de cœurs cristallisent beaucoup d'activités scientifiques autour du calcul hautes performances. Ces travaux répondent à un besoin en information et en formation de la part de chercheurs et d'ingénieurs qui veulent positionner un large spectre de travaux de recherche vis à vis de ces architectures. Aujourd'hui, il s'agit des processeurs graphiques (GPU) mais les industriels travaillent sur de nombreuses autres solutions.
Nous observons que les recherches actuelles portent principalement sur la réalisation de prototypes utilisant des GPU pour accélérer des applications généralement exécutées sur des processeurs généralistes — GPGPU [GLGN+08]. Ces travaux remettent à jour nombre de problèmes rencontrés par le passé avec les architectures massivement parallèles ou exotiques. Nous considérerons donc ces architectures et leurs environnements dans un contexte plus large où elles ne sont qu'une étape vers de futures architectures multi-cœur hétérogènes.

Résultats obtenus. Parmi les diverses problématiques liées à l'utilisation de processeurs graphiques pour l'accélération d'applications généralistes, nous nous sommes concentrés sur les outils de simulation, le transfert d'applicatif, l'étude de la consommation et la gestion du parallélisme de données.
La structure interne des GPU est largement inconnue et les compteurs de performance, habituellement disponibles dans les architectures classiques, ne sont pas ou peu accessibles. Cette absence contraint (trop) fortement les développeurs dans les optimisations pour ces architectures. C'est la raison pour laquelle nous travaillons sur un simulateur de processeur graphique Barra[90]. Ce simulateur s'appuie sur divers travaux conduits au sein de l'équipe et destinés à mieux comprendre le fonctionnement des GPU [**?**, 69].
Les calculs réalisés par ces processeurs graphiques utilisent principalement l'arithmétique flottante. Cependant nous avons montré en quoi l'arithmétique implémentée ne se conforme pas à la norme IEEE-754 [3]. Pour certaines applications, ce problème est rédhibitoire. Nous avons donc proposé une bibliothèque d'opérateurs d'arithmétique par intervalle optimisée pour GPU [31].
Les GPU sont réputés pour être énergivore avec des consommations pouvant atteindre 300 Watts. Dans le contexte actuel de réduction de la consommation énergétique, nous nous sommes intéressés à mesurer la consommation de ces processeurs afin de pouvoir la modéliser et intégrer un modèle de consommation dans le simulateur Barra [29].

Travaux en cours. Nous poursuivons le développement du simulateur Barra selon deux directions. D'une part nous affinons la précision et l'étendue du simulateur par rapport aux GPU existants. D'autre part, nous exploitons les versions successives de Barra pour évaluer les nouvelles évolutions matérielles de GPU que nous proposons.

2.3 Action 3. Nouveaux algorithmes précis, validés et rapides

Contexte et originalité de l'approche. La précision du résultat d'un calcul en précision finie dépend de trois facteurs : le conditionnement du problème à résoudre, la stabilité de l'algorithme numérique et la précision de l'arithmétique utilisée. Cette dernière est souvent l'arithmétique flottante binaire IEEE-754 qui ne permet pas de calculer une solution précise de problèmes mal conditionnés.
La parade classique consiste à implanter ces algorithmes avec des bibliothèques de précision arbitraire [Bai],[MPF], ou — seulement — étendue lorsque la vitesse des calculs est cruciale. Les réalisations

[GLGN+08] Michael Garland, Scott Le Grand, John Nickolls, Joshua Anderson, Jim Hardwick, Scott Morton, Everett Phillips, Yao Zhang, and Vasily Volkov. Parallel computing experiences with cuda. *IEEE Micro*, 28(4):13–27, 2008.

[Bai] High-precision software directory. URL = `http://crd.lbl.gov/~dhbailey/mpdist`.

[MPF] The MPFR library. URL = `http://www.mpfr.org/`.

les plus abouties[LDB+02] en ce sens sont les bibliothèques "double-double" et "quad-double" qui implantent respectivement deux ou quatre fois la double précision IEEE [Bai].

L'originalité de l'approche suivie est l'étroite association entre les méthodes numériques d'analyse d'erreur et les propriétés fines de l'arithmétique en précision finie[Lan01,Lan04]. L'utilisation de "transformations sans erreurs"[ORO05] nous permet de prouver l'amélioration de précision. Ainsi nous proposons des algorithmes, les preuves et les logiciels associés qui produisent, en utilisant uniquement l'arithmétique IEEE-754, des solutions calculées plus précises, des bornes d'erreurs significatives et validées, et ce avec des performances de calcul compétitives sur les machines actuelles.

Résultats obtenus. Nous avons introduit des algorithmes compensés pour l'évaluation polynomiale et la résolution de systèmes linéaires triangulaires [47, 97]. Pour l'évaluation polynomiale en particulier, ces algorithmes produisent des résultats arbitrairement précis et assortis des bornes de validité, statique ou dynamique, sur l'erreur résiduelle ; le tout en n'utilisant que l'arithmétique flottante IEEE-754 [11]. Nous avons entre autres étudié l'effet des opérateurs arithmétiques ainsi que l'arrondi correct de cette évaluation [41, 47].
Les algorithmes compensés qui doublent ou quadruple la précision de calcul sont plus performants que les solutions alternatives citées plus haut — au moins deux fois plus rapides en termes de vitesse de calcul. Nous avons montré que de telles performances étaient justifiées par un important parallélisme d'instruction de ces algorithmes, propriété exploitée par les architectures superscalaires actuelles [97].

Travaux en cours. L'analyse de la rapidité mesurée de ces algorithmes précis que nous avons proposé répond à une question ouverte pour l'addition et le produit scalaire précis[ORO05]. Nous confortons actuellement cette analyse par le biais de simulations de l'exécution de ces algorithmes sur un processeur idéal[HP03]. Il apparaît que ces algorithmes compensés disposent d'un potentiel d'exécution rapide non encore exploité par les processeurs superscalaires actuels [19].

2.4 Action 4 : Certification et applications

Contexte et originalité de l'approche. La certification des applications qui calculent en précision finie est une nécessité. Les méthodes et les outils de certification sont variés (arithmétique d'intervalle, symbolique-numérique, preuve formelle, analyse statique) et dépendent fortement de la taille des codes et des domaines d'application. Deux approches ont été considérées dans cette voie. L'une, assez spécialisée et maintenant en sommeil, exploite la notion de pseudo-zéros de polynôme pour certifier, entre autres, la stabilité de problèmes de la théorie du contrôle.

Le recrutement en 2007 d'un MCF HDR a permis d'orienter cette certification vers des applications de dimension plus industrielles : les traitements numériques réalisés par des systèmes embarqués critiques tels que, par exemple, le système de contrôle-commande numérique d'un avion. Pour cela, on étudie des techniques de validation et de transformation des calculs présents dans ces applications avec pour objectifs de majorer les erreurs d'arrondi dans des codes de grande taille, d'optimiser des programmes vis-à-vis de la précision numérique et de développer des outils automatiques et

[LDB+02] Xiaoye S. Li, James W. Demmel, David H. Bailey, Greg Henry, Yozo Hida, Jummy Iskandar, William Kahan, Suh Y. Kang, Anil Kapur, Michael C. Martin, Brandon J. Thompson, Teresa Tung, and Daniel J. Yoo. Design, implementation and testing of extended and mixed precision BLAS. *ACM Transactions on Mathematical Software*, 28(2):152–205, June 2002.

[Bai] High-precision software directory. URL = `http://crd.lbl.gov/~dhbailey/mpdist`.

[Lan01] Philippe Langlois. Automatic linear correction of rounding errors. *BIT*, 41(3):515–539, September 2001.

[Lan04] Philippe Langlois. More accuracy at fixed precision. *J. Comp. Appl. Math.*, 162(1):57–77, January 2004.

[ORO05] Takeshi Ogita, Siegfried M. Rump, and Shin'ichi Oishi. Accurate sum and dot product. *SIAM J. Sci. Comput.*, 26(6):1955–1988, 2005.

[HP03] John L. Hennessy and David A. Patterson. *Computer Architecture – A Quantitative Approach*. Morgan Kaufmann, 2nd edition, 2003.

utilisables industriellement. D'un point de vue théorique, ces travaux s'appuient sur des méthodes d'analyse statique de programmes par interprétation abstraite[CC77].

Résultats obtenus. Dans un premier temps, nous avons approfondi la connaissance des pseudo-zéros de polynômes, notion ancienne[Mos86] mais peu utilisée jusqu'à présent. Nous avions adapté cette notion à la prise en compte des perturbations effectives introduites par l'arithmétique flottante sur les coefficients [GL04]. Nous avons ensuite étendu ces pseudo-zéros à des polynômes d'intervalles [37]. Enfin nous proposons des algorithmes symboliques-numériques qui calculent de façon certifiée le rayon de stabilité et la pseudo-abscisse d'un polynôme ; ce qui répond à des problèmes de stabilité en théorie du contrôle [10].

L'approche de certification actuellement développée s'appuie donc sur les méthodes d'analyse statique de programmes par interprétation abstraite. Nous détectons ainsi les pertes de précision numérique dues à l'utilisation des nombres flottants [13]. D'autre part, nous nous intéressons aux techniques de transformation sémantique de programmes afin d'en améliorer la qualité des calculs [14, 52]. La sûreté des traitements numériques réalisés par des systèmes embarqués critiques a nécessité l'étude de sujets connexes, notamment à travers les deux thèses (préparées hors équipe) soutenues en 2008[Bou08,Cha08]. Nous avons considéré les systèmes hybrides discrets-continus (pour modéliser l'environnement physique dans lequel évolue un système embarqué) et les systèmes synchrones (tels que SCADE ou Simulink, très souvent employés dans l'industrie pour spécifier des systèmes embarqués) [22, 23, 2, 25].

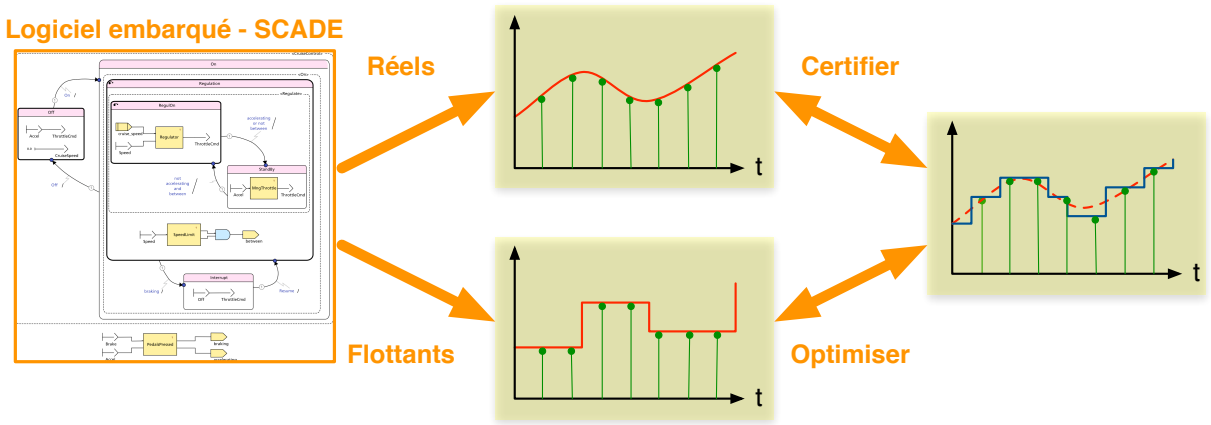

FIG. 2 – *Les objectifs de l'action "certification et applications".*

Travaux en cours. Actuellement, un outil d'analyse et de transformation de programmes est en cours de développement. Il regroupe les principaux résultats de cette action. Comme l'illustre la figure 2, ce logiciel a pour but de permettre de certifier et optimiser des logiciels critiques issus de systèmes embarqués industriels : on considère, d'une part, une description de haut niveau d'un logiciel (en SCADE par exemple), dans laquelle les calculs sont supposés exacts et, d'autre part, l'implémentation du même logiciel, dans laquelle les résultats des calculs sont arrondis. La certification consiste à borner, pour toutes les exécutions possibles, l'écart entre les deux calculs. L'opti-

[CC77] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977. ACM Press, New York, NY.

[Mos86] Ronald G. Mosier. Root neighborhoods of a polynomial. *Math. Comp.*, 47(175):265–273, 1986.

[GL04] Stef Graillat and Philippe Langlois. A comparison of real and complex pseudozero sets for polynomials with real coefficients. In Christiane Frougny et al., editors, *RNC-6, Real Numbers and Computer Conference, Schloss Dagstuhl, Germany*, pages 103–112, November 2004.

[Bou08] Olivier Bouissou. *Interprétation abstraite de systèmes hybrides*. Doctorat en informatique, Ecole Polytechnique, 2008.

[Cha08] Alexandre Chapoutot. *Interprétation abstraite de Simulink*. Doctorat en informatique, Ecole Polytechnique, 2008.

misation consiste à transformer l'implémentation afin de se rapprocher des résultats théoriques. Ce travail est soutenu par la Fondation pour la Recherche en Aéronautique et l'Espace (FNRAE).

2.5 Action 5 : Opérateurs arithmétiques pour la cryptographie

Contexte et originalité de l'approche. La cryptographie sert pour l'essentiel à garantir la confidentialité des communications et à authentifier des données et des personnes. Divers protocoles cryptographiques nécessitent des opérations arithmétiques efficaces et sûres. En effet, deux des cryptosystèmes les plus utilisés sont RSA et ECC. Pour RSA, la plupart des protocoles nécessitent une exponentiation modulo un entier. Cette exponentiation s'effectue en une série de multiplications et de carrés modulaires. De même l'implantation de protocoles basés sur les courbes elliptiques, nécessite une chaîne relativement longue d'opérations dans un corps finis. Ces corps finis sont soit des corps binaires, soit des corps premiers, soit des corps $GF(p^k)$ (ces derniers étant surtout utilisés dans les protocoles basés sur les couplages). L'arithmétique dans ces corps finis se ramène en général a une arithmétique entière modulaire et polynomiale.

Résultats obtenus. Nous proposons de nouvelles approches pour l'arithmétique dans les corps finis ainsi que des travaux sur l'amélioration de l'arithmétique sur des classes de courbes elliptiques. Concernant les corps finis, nous proposons divers algorithmes et architectures pour effectuer une multiplication dans des corps binaires. Nous introduisons entre autres deux approches exploitant une structure Toeplitz [43, 42]. Par ailleurs nous définissons une nouvelle représentation des corps binaires permettant l'utilisation de la FFT pour la multiplication [60, 88]. Nous utilisons aussi l'approche FFT en exploitant une représentation des entiers modulaires[Pla05] [58]. Cette stratégie est aussi développée pour les corps $GF(p^k)$ [36].
Sur l'arithmétique des courbes, nous proposons une nouvelle représentation des points sur certaines courbes elliptiques en caractéristique 3. Cette représentation permet d'améliorer les opérations élémentaires sur la courbe comme le triplement et l'addition [44, 55].

Travaux en cours. En collaboration avec A. Hasan (Univ. Waterloo) Nous construisons un nouveau type de multiplieur qui combine l'approche parallèle et séquentielle (multiplieur séquentiel sous-linéaire en espace). Nous améliorons certains algorithmes de multiplication dans $\mathbb{F}_{p^k}$ en étendant le travail effectué pour les corps $GF(p^k)$ grâce à d'autres représentations de p. En collaboration avec N. Méloni (Université Waterloo, Canada), nous proposons une solution algorithme/architecture qui améliore le hachage dans GCM. Ce travail s'appuie sur un calcul astucieux du polynôme minimal mis en jeu.

[Pla05] Thomas Plantard. *Arithmétique modulaire pour la cryptographie*. Doctorat en informatique, Université Montpellier 2, December 2005.

3 Production scientifique et reconnaissance

3.1 Production scientifique

Publications. Le tableau suivant présente les publications des membres de l'équipe DALI en se limitant à celles produites au sein de l'équipe (à la différence de la liste des publications présentée en section 4 selon les recommandations de l'AERES : "Pour les membres recrutés au cours des quatre dernières années, les publications effectuées dans leur unité d'origine pourront être citées".) De même, nous séparons les publications internationales des autres productions.

	2005	2006	2007	2008	*ratio 05-08*
# permanents	3	5	6	7	7
Journaux internat. (ACLi)	3	3	3	3	*0.57*
Actes intern. sélect. (ACTIs)	3	9	12	10	*1.62*
Invitations intern. (INV)		1		1	*0.10*
Ratio international (CNRS)					**2.29**
Journaux nat. (ACLn)		1		2	*0.14*
Invitations nat. (INVn)	1		1	1	*0.14*

Logiciels.

Barra est un simulateur de processeur graphique NVIDIA développé par S. Collange, D. Defour et D. Parello depuis le début de l'année 2009. Il est basé sur l'environnement de simulation UNISIM[3]. Il permet d'exécuter du code NVIDIA CUDA pour en extraire des statistiques permettant l'optimisation autant au niveau logiciel que matériel.

Boost.Interval-GPU est est une bibliothèque d'arithmétique d'intervalle sur GPU en C++ basée sur la bibliothèques Boost.Interval. Elle est développée et maintenue par S. Collange, M. Daumas et D. Defour depuis 2008, et est utilisée au GIlab à l'Université de Gérone (Espagne) pour une application de lancer de rayon certifié sur surfaces implicites.

Fluctuat-assembleur est un logiciel d'analyse statique de programmes développé par M. Martel au CEA (depuis 2003) puis à l'Université de Perpignan (depuis 2007), en collaboration avec Airbus. Il est destiné à valider la précision des calculs effectués dans des codes embarqués critiques écrits en assembleur pour le processeur TMS-320 de Texas Instruments.

OOSim est un simulateur modulaire au niveau cycle de processeur super-scalaire générique basé sur le jeu d'instruction PowerPC. Très paramétrable et très modulaire, il permet de simuler aussi bien une micro-architecture idéale que la micro-architecture représentative des microprocesseurs actuels. Il est développé et maintenu par D. Parello dans UNISIM , environnement de simulation modulaire offrant une librairie de composants et de simulateurs. OoOSim est donc disponible sous licence BSD à partir de la librairie de composants UNISIM.

3.2 Docteurs et doctorants

3.2.1 Les deux premiers docteurs immédiatement recrutés comme MCF

Bilan. Sur la période concernée, deux thèses entièrement préparées dans l'équipe ont été soutenues. En novembre 2005, S. Graillat soutient **la première thèse en informatique de l'UPVD**. En novembre 2007, N. Louvet soutient la deuxième. L'un et l'autre sont ensuite recrutés comme maître de conférences dans les meilleures équipes de recherche du domaine.

[3]UNISIM est une plate forme de simulation fédérant de nombreux instituts : INRIA Scalay, CEA List, Princeton University, Universitat Politècnica de Catalunya, Barcelona Supercomputing Center, Ghent University, Brigham Young University, Université de Perpignan, ARM, ST Microelectronics. `www.unisim.org`

S. Graillat. "Fiabilité des algorithmes numériques : pseudo-solutions structurées et précision". Allocataire normalien 2003-2005, direction : Ph. Langlois ; novembre 2005 : soutenance ;
septembre 2006 : MCF à l'Université Paris 6, équipe CALCOMP au LIP6.

N. Louvet. "Algorithmes compensés en arithmétique flottante : précision, validation, performances". Allocataire ACI JC 2005-2007, direction : Ph. Langlois ; novembre 2007 : soutenance ;
septembre 2008 : MCF à l'Université Lyon 1, membre du projet Arénaire au LIP.

3.2.2 Doctorants actuellement au sein de DALI

M. Bouache. "Simulation de processeurs hautes performances". financement Université Boumerdès (Algérie), ERASMUS, direction : B. Goossens, D. Parello ; soutenance prévue fin 2010.

S. Collange. "GPGPU". Allocataire ED E2 (UPVD), direction : M. Daumas, D. Defour ; soutenance prévue fin 2010.

A. El Moussaoui. "Traitement parallèle des instructions". Financement BCU, Amer. Univ. Liban, direction : B. Goossens, D. Parello ; soutenance prévue 2011.

C. Ke. "Extraction parallèle des instructions". Financement société "véhicules urbains", Chine, direction : B. Goossens, D. Parello ; soutenance prévue fin 2011.

3.2.3 Autres encadrements de doctorants par des membres de l'équipe

O. Bouissou."Interprétation abstraite de systèmes hybrides". Direction M. Martel ; soutenance en septembre 2008, École Polytechnique.

A. Chapoutot. "Interprétation abstraite de Simulink". Direction M. Martel ; soutenance en décembre 2008, École Polytechnique.

3.3 Contrats ou programmes de recherche financés hors budget récurrent

BioWic : Workflow pour les traitements intensifs en bioinformatique
– Partenaires : CAIRN/INRIA, UPVD, MIG/INRA, Ouest Génopole, Symbios, INRIA Rennes
– Cadre et durée : projet ANR Calcul intensif 2009-2011
– Financement : 75 k€

EVAFlo : Évaluation et Validation Automatique pour le Flottant
– Partenaires : ENS Lyon, UPVD, CEA
– Cadre et durée : projet ANR Blanc 2006-2010
– Financement : 35 k€

GP-GPU : collaboration et veille technologique
– Partenaires : Nvidia, ATI
– Cadre et durée : donation de matériel 2007-2009
– Financement : 18 k€

GP-GPU : nouvelles architectures pour le calcul scientifique
– Partenaire : Groupe énergétique français
– Cadre et durée : convention Polytech'Paris 2008
– Financement : 20 k€

MASSANES : développement d'un outil pour la validation de systèmes de commandes de vol numériques
– Partenaires : Airbus et CEA
– Cadre et durée : Dir. des Programmes de l'Aviation Civile, 2007-2008
– Financement : 35k€

SARDANES : transformation certifiée de codes SCADE pour la précision numérique
– Partenaires : ENS et UBO
– Cadre et durée : Fondation Aéronautique et Espace, 2009-2012
– Financement : 300k€

3.4 Reconnaissance, visibilité internationale et nationale

3.4.1 Reconnaissance internationale

Conférencier invité dans des conférences internationales
– SCAN 2006 : Scientific Computing and Applied Numerics, Duisburg, Allemagne
– NSV 2008 : International Workshop on Numerical Abstraction for Software Validation, Princeton, Etats-Unis
– INVA'09 : International Workshop of Validated Algorithms, Miyakojima, Japon

3.4.2 Implication dans la vie de la communauté

Actions d'animation scientifique internationale et nationale
– 17th International Static Analysis Symposium : organisation du SAS'10 à Perpignan en 2010
– 21th ACM Symposium on Applied Computing, Dijon, 2006 : co-organisation, avec S.M. Rump, de la session *More accurate computation : methods and software*
– Journées Thème Emergent CNRS : co-organisation et gestion d'une action nationale GPU-Manycore (GDR ASR), 2008-09
– Cours dans les écoles thématiques ARCHI05, 07, 09 et RAIM'08
– Organisation de la conférence Sympa'06, Canet-en-roussillon
– Organisation des journées Arinews, Perpignan, 2005
– Participation au jury du prix SPECIF des "Meilleures thèses en informatique" (04-06)

3.4.3 Actions et collaborations scientifiques

Collaborations internationales en cours
– A. Hasan à Université de Waterloo, Canada : opérateurs cryptographiques et courbes elliptiques
– W. Taha à Rice University, US : simulation certifiée de processus physiques
– Esterel Technologies et Airbus : développement d'un logiciel d'analyse et transformation pour SCADE
– S. Oishi et S.M. Rump à Waseda University, Tokyo : algorithmes numériques précis et validés
– J.-L. Gaudiot à U. California Irvine, US : processeurs haute-performances
– M. Mezghiche, Université Boumerdès, Algérie : processeurs haute-performances

3.4.4 Animation interne, visibilité et "vécu" DALI-LIRMM

Voir `http://webdali.univ-perp.fr`
Professeurs invités : 1-2 mois par an depuis 2006.
Séminaire équipe DALI : depuis 2003 (15 séances depuis septembre 2008 dont 13 intervenants extérieurs).
Master informatique de l'UM2 : un cours renouvelé chaque année depuis 2004.
Actions antérieures : commissions de spécialistes 27ème section de l'UPVD (depuis 2004), de l'UM3 ; Comité d'Orientation Scientifique Technique et Industriel (département TIC) de la Région LR.
Intégrations croisées entre DALI et le LIRMM : Ch. Nègre, P. Giorgi.

4 Liste des publications sur la période 2005-2009

4.1 Articles dans des revues internationales ou nationales répertoriées

[1] N. Brisebarre, D. Defour, P. Kornerup, J.-M. Muller, and N. Revol. A new range-reduction algorithm. *IEEE Trans. Computers*, 54(3) :331–339, 2005.

[2] A. Chapoutot and M. Martel. Différentiation automatique et formes de taylor en analyse statique de programmes numériques. *Journal des Techniques et Sciences Informatiques (TSI)*, pages 503–531, 2009.

[3] S. Collange, M. Daumas, and D. Defour. Etat de l'intégration de la virgule flottante dans les processeurs graphiques. *Revue des sciences et technologies de l'information*, 27/6 :719–733, 2008.

[4] S. Collange, M. Daumas, and D. Defour. Line-by-line spectroscopic simulations on graphics processing units. *Computer Physics Communications*, 178 :135–143, January 2008.

[5] J.-G. Dumas, P. Giorgi, and C. Pernet. Dense linear algebra over word-size prime fields : the fflas and ffpack packages. *ACM Trans. Math. Softw.*, 35(3) :1–42, 2008.

[6] B. Goossens and D. Defour. The instruction register file micro-architecture. *Future Generation Comp. Syst.*, 21(4) :767–773, 2005.

[7] B. Goossens and D. Defour. Ordonnancement distribué d'instructions. *Technique et Science Informatiques*, 25(7) :827–844, 2006.

[8] S. Graillat. A note on a nearest polynomial with a given root. *SIGSAM Bull.*, 39(2) :53–60, 2005.

[9] S. Graillat. A note on structured pseudospectra. *J. Comput. Appl. Math.*, 191(1) :68–76, 2006.

[10] S. Graillat and P. Langlois. Real and complex pseudozero sets for polynomials with applications. *Theor. Inform. Appl.*, 41(1) :45–56, 2007.

[11] S. Graillat, P. Langlois, and N. Louvet. Algorithms for accurate, validated and fast computations with polynomials. *Japan Journal of Industrial and Applied Mathematics*, Special issue on Verified Numerical Computation. 26(2–3), 2009. (To appear).

[12] J.-C.Bajard, L. Imbert, and C. Negre. Arithmetic operations in finite fields of medium prime characteristic using lagrange representation. *IEEE trans. comp.*, 55(9) :1167–1177, sept 2006.

[13] M. Martel. Semantics of roundoff error propagation in finite precision computations. *Journal of Higher Order and Symbolic Computation*, pages 7–30, 2006.

[14] M. Martel. Enhancing the implementation of mathematical formulas for fixed-point and floating-point arithmetics. *Journal of Formal Methods in System Design*, 2009. To appear (15 pages).

[15] C. Negre. Efficient parallel multiplier in shifted polynomial basis. *Journal of Systems Architecture*, 53(2-3) :109–116, 2007.

[16] C. Negre. Finite field arithmetic using quasi-normal basis. *Finite Fields and Their Applications*, 13 :635–647, 2007.

[17] G. Sylvain, V. Nicolas, B. Cédric, C. Albert, P. David, S. Marc, and T. Olivier. Semi-automatic composition of loop transformations for deep parallelism and memory hierarchies. *Int. J. Parallel Program.*, 34(3) :261–317, 2006.

4.2 Conférences données à l'invitation du comité d'organisation d'une conférence internationale (INV)

[18] P. Langlois. Compensated algorithms in floating point arithmetic. In *12th GAMM - IMACS International Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics, Duisburg, Germany*, September 2006. (Invited plenary speaker).

[19] P. Langlois. Performance analysis of some accurate and validated algorithms. In *International Workshop on Verified Numerical Computations and its Applications, INVA'09, Miyakojima, Japon*, March 2009. (Invited speaker).

[20] M. Martel. Enhancing the implementation of mathematical formulas for fixed-point and floating-point arithmetics. In *International Workshop on Numerical Abstractions for Software Verification*, 2008. (Invited paper).

4.3 Communications avec actes dans des conférences internationales (ACTI)

[21] J.-C. Bajard, P. Langlois, D. Michelucci, G. Morin, and N. Revol. Floating-point geometry : toward guaranteed geometric computations with approximate arithmetics. In *Proc. SPIE*, volume 7074, page 10, August 2008.

[22] O. Bouissou and M. Martel. Grklib : a guaranteed runge-kutta library. In *Proceedings of the 12th GAMM - IMACS International Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics, Duisburg, Germany*. IEEE Conference Proceedings, 2007.

[23] O. Bouissou and M. Martel. Abstract interpretation of the physical inputs of embedded programs. In *Verification, Model Checking, and Abstract Interpretation (VMCAI), 9th International Conference*, number 4905 in Lecture Notes in Computer Science, pages 37–51, 2008.

[24] O. Bouissou and M. Martel. A hybrid denotational semantics for hybrid systems. In *17th European Symposium on Programming (ESOP)*, number 4960 in Lecture Notes in Computer Science, pages 63–77, 2008.

[25] A. Chapoutot and M. Martel. Abstract simulation : a static analysis of simulink models. In *6th IEEE International Conference on Embedded Systems and Software, ICESS'09*. IEEE Press, 2009. To appear (10 pages).

[26] A. Cohen, M. Sigler, S. Girbal, O. Temam, D. Parello, and N. Vasilache. Facilitating the search for compositions of program transformations. In *ICS '05 : Proceedings of the 19th annual international conference on Supercomputing*, pages 151–160, Cambridge, Massachusetts, 2005. ACM Press.

[27] S. Collange, Y. S. Dandass, M. Daumas, and D. Defour. Using graphics processors for parallelizing hash-based data carving. In *HICCS, Hawaii International Conference on System Sciences*, pages 1–10, 2009.

[28] S. Collange, M. Daumas, and D. Defour. Graphic processors to speed-up simulations for the design of high performance solar receptors. In *IEEE 18th International Conference Application-specific Systems, Architectures and Processors*, pages 377–382, Montréal Canada, 2007. IEEE.

[29] S. Collange, D. Defour, and A. Tisserand. Power consuption of gpus from a software perspective. In *ICCS 2009 : Compute.Discover.Innovate.*, volume 5544 of *Lecture Notes in Computer Science*, pages 922–931. Springer, 2009.

[30] S. Collange, J. Detrey, and F. de Dinechin. Floating point or lns : Choosing the right arithmetic on an application basis. In *Euromicro Conference on Digital System Design*, pages 197–203, Los Alamitos, CA, USA, 2006. IEEE Computer Society.

[31] S. Collange, J. Flóres, and D. Defour. A gpu interval library based on boost interval. In *RNC9, Real Numbers and Computers*, pages 61–72, Jully 2008.

[32] A. Costan, E. Goubault, S. Gaubert, M. Martel, and S. Putot. A policy iteration algorithm for computing fixed points in static analysis of programs. In *Computer Aided Verification, CAV'05*, number 3576 in Lecture Notes in Computer Science, pages 462–475. Springer-Verlag, 2005.

[33] G. Da Graça and D. Defour. Implementation of float-float operators on graphics hardware. In *RNC7*, pages 23–32, July 2006.

[34] D. Defour. Collapsing dependent floating point operations. In *IMACS World Congress Scientific Computation, Applied Mathematics and Simulation*, pages 1–10, Paris, France, July 2005.

[35] W. Eberly, M. Giesbrecht, P. Giorgi, A. Storjohann, and G. Villard. Solving sparse rational linear systems. In *ISSAC '06 : Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 63–70, New York, NY, USA, 2006. ACM.

[36] N. El Mrabet and C. Negre. Finite field multiplication combining amns and dft approach for pairing cryptography. In *Proceedings of Australasian Conference on Information Security and Privacy (ACISPP 09)*, 2009. (to appear).

[37] S. Graillat and P. Langlois. Pseudozero set of interval polynomials. In *Proceedings of the 21st Annual ACM Symposium on Applied Computing*, volume 2, pages 1655–1659. Association for Computing Machinery, April 2006.

[38] S. Graillat, P. Langlois, and N. Louvet. Accurate dot products with fma. In G. Hanrot and P. Zimmermann, editors, *RNC-7, Real Numbers and Computer Conference, Nancy, France*, pages 141–142, July 2006. Extended version available on-line.

[39] S. Graillat, P. Langlois, and N. Louvet. Choosing a twice more accurate dot product implementation. In *International Conference of Numerical Analysis and Applied Mathematics 2006, Hersonnisos, Crete, Greece*, pages 498–499, September 2006.

[40] S. Graillat, P. Langlois, and N. Louvet. Fused multiply and add implementations of the compensated horner scheme. In P. Hertling, C. Hoffmann, W. Luther, and N. Revol, editors, *Reliable Implementation of Real Number Algorithms : Theory and Practice*, Dagstuhl Seminar 6021, January 2006. Extended version available on-line.

[41] S. Graillat, P. Langlois, and N. Louvet. Improving the compensated horner scheme with a fused multiply and add. In *Proceedings of the 21st Annual ACM Symposium on Applied Computing*, volume 2, pages 1323–1327. Association for Computing Machinery, April 2006.

[42] A. Hasan and C. Negre. Subquadratic space complexity multiplication over binary fields with dickson polynomial representation. In *Proceedings of WAIFI 2008, Sienna, Italy*, volume 5130 of *LNCS*, pages 88–102, 2008.

[43] A. Hasan and C. Negre. Subquadratic space complexity multiplier for a class of finite fields using toeplitz matrix approach. In *ARITH 19, 19th IEEE Symposium on Computer Arithmetic*, 2009. (to appear).

[44] K.-H. Kim and C. Negre. Point multiplication on supersingular elliptic curves defined over fields of characteristic 2 and 3. In *SECRYPT'08, Porto, Portugal*, pages 373–376, 2008.

[45] P. Langlois, S. Graillat, and N. Louvet. Compensated horner scheme. In B. Buchberger, S. Oishi, M. Plum, and S. M. Rump, editors, *Algebraic and Numerical Algorithms and Computer-assisted Proofs*, number 05391 in Dagstuhl Seminar Proceedings, pages 1–29. Internationales Begegnungs- und Forschungszentrum (IBFI), Schloss Dagstuhl, Germany, 2006.

[46] P. Langlois and N. Louvet. Solving triangular systems more accurately and efficiently. In *Proceedings of the 17th IMACS World Congress, Paris*, volume CD-ROM, pages 1–10, July 2005.

[47] P. Langlois and N. Louvet. How to ensure a faithful polynomial evaluation with the compensated horner algorithm ? In P. Kornerup and J.-M. Muller, editors, *ARITH'18, 18th IEEE International Symposium on Computer Arithmetic*, number ISBN 0-7695-2854-6, pages 141–149. IEEE Computer Society, June 2007.

[48] P. Langlois and N. Louvet. Operator dependant compensated algorithms. In *Proceedings of the 12th GAMM - IMACS International Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics, Duisburg, Germany*. IEEE Conference Proceedings, 2007. 11 pages.

[49] P. Langlois and N. Louvet. Compensated horner algorithm in k times the working precision. In J. Brugera and M. Daumas, editors, *RNC-8, Real Numbers and Computer Conference, Santiago de Compostela, Spain*, pages 157–166, July 2008.

[50] M. Martel. An overview of semantics for the validation of numerical programs. In *Verification, Model Checking and Abstract Interpretation, VMCAI'05*, number 3385 in Lecture Notes in Computer Science, pages 59–77. Springer-Verlag, 2007.

[51] M. Martel. Semantics-based transformation of arithmetic expressions. In *Static Analysis Symposium, SAS'07*, number 4634 in Lecture Notes in Computer Science, pages 298–314. Springer-Verlag, 2007.

[52] M. Martel. Program transformation for numerical precision. In *ACM Workshop on Partial Evaluation and Program Manipulation, PEPM'09*, pages 101–109. ACM Press, 2009.

[53] C. Negre. Exponentiation to the power p in gf(p^k) using variants of montgomery modular arithmetic. In *Proceedings of Nordsec 2005, Tartu Estonia*, pages 71–83, October 2005.

[54] C. Negre. Quadrinomial modular multiplication using modified polynomial basis. In *Proceedings of ITCC 2005, Las Vegas USA*, volume 1 of *LNCS*, pages 550–555, April 2005.

[55] C. Negre. Scalar multiplication on elliptic curves defined over fields of small odd characteristic. In *Indocrypt 2005, Bangalore India*, volume 3797 of *LNCS*, pages 389–402, December 2005.

[56] C. Negre. Finite field multiplication in lagrange represenation using fast fourrier transform. In *SECRYPT'06,Setúbal,Portugal*, pages 320–323, August 2006.

[57] C. Negre. Parallel multiplication in gf(2^n) using condensed matrix representation. In *SECRYPT'06, Setúbal,Portugal*, pages 254–259, August 2006.

[58] C. Negre and T. Plantard. Efficient modular arithmetic in adapted modular number system using lagrange representation. In *Proceedings of Australasian Conference on Information Security and Privacy (ACISPP 08)*, volume 5107 of *LNCS*, pages 463–477, 2008.

[59] D. Parello, M. Bouache, and B. Goossens. Improving cycle-level modular simulation by vectorization. In *Rapid Simulation and Performance Evaluation : Methods and Tools (RAPIDO'09), Held in conjunction with the 4th International Conference on High-Performance and Embedded Architectures and Compilers (HiPEAC)*, page 6, Paphos Cyprus, 2009.

[60] P.Giorgi, C. Negre, and T. Plantard. Subquadratic binary field multiplier in double polynomial system. In *SECRYPT'07, Barcelona, Spain*, pages 229–236, 2007.

[61] B. Senouci, M. Bouache, and B. Goossens. Bridging processor elements in heterogeneous mpsoc : A hardware oriented approach. In *Proceedings of High Performance Computing and Simulation conference (HPCS'09), Leipzig, Germany*, June 2009. (To appear).

[62] B. Senouci, M. Bouache, and B. Goossens. Heterogeneous multi-processor soc design : Hardware bridging and exploration methodology. In *Proceedings of the International conference in Embedded System and Application (ESA'09), Las Vegas, USA*, July 2009. (To appear).

[63] P. Vouzis, M. Arnold, S. Collange, and M. Kothare. Monte carlo logarithmic number system for model predictive control. In *Field Programmable Logic and Applications, 2007. FPL 2007. International Conference on*, pages 453–458, 2007.

[64] P. Vouzis, S. Collange, and M. Arnold. Lns subtraction using novel cotransformation and/or interpolation. In *IEEE 18th International Conference Application-specific Systems, Architectures and Processors*, pages 107–114, July 2007.

[65] P. D. Vouzis, S. Collange, and M. G. Arnold. Cotransformation provides area and accuracy improvement in an hdl library for lns subtraction. In *Euromicro Conference on Digital System Design*, pages 85–93, Los Alamitos, CA, USA, 2007. IEEE Computer Society.

[66] Y.Li and C. Negre. An efficient multiplication algorithm using binomial residue representation. In *SECRYPT'08, Porto, Portugal*, pages 319–324, 2008.

[67] A. Yun Zhu, W. Taha, C. Cartwright, M. Martel, and J. Siek. In pursuit of real answers. In *6th IEEE International Conference on Embedded Systems and Software, ICESS'09*. IEEE Press, 2009. To appear (10 pages).

4.4 Communications avec actes dans des conférences nationales (ACTN)

[68] A. Chapoutot and M. Martel. Différentiation automatique et formes de taylor en analyse statique de programmes numériques. In *10ième conférence francophone sur les Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL)*, pages 261–277, 2007.

[69] S. Collange, M. Daumas, D. Defour, and R. Olivès. Fonctions élémentaires sur gpu exploitant la localité de valeurs. In *SympA*, pages 1–11, February 2008.

[70] M. Daumas, G. Da Graça, and D. Defour. Caractéristiques arthmétiques des processeurs graphiques. In *SympA*, pages 86–95, october 2006.

[71] B. Goossens and D. Defour. Ordonnancement dynamique distribué. In *SympA*, pages 1–10, 2005.

[72] D. Parello, M. Bouache, B. Goossens, and A. E. Moussaoui. Comment répartir les ressources du chemin de données ? In *Proceedings of Perpi'2006 - Conférences conjointes RenPar'17 / SympA'2006 / CFSE'5 / JC'2006.*, pages 12–23, Canet en Roussillon, 2006.

4.5 Communications orales sans actes dans des conférences (COM)

[73] O. Bouissou and M. Martel. A runge-kutta method for computing guaranteed solutions of odes. In *12th GAMM - IMACS International Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics, SCAN'06, Duisburg, Germany*, 2006.

[74] A. Chapoutot and M. Martel. Static analysis of simulink programs. In *SLA++P'08, Model-driven High-level Programming of embedded Systems*, 2008.

[75] E. Goubault, M. Martel, and S. Putot. Some future challenges in the validation of control systems. In *European Congress on Embedded Real Time Software (ERTS)*, 2006.

[76] P. Langlois. Compensated algorithms and validated bounds. SWIM 08, Montpellier, June 2008.

[77] P. Langlois and N. Louvet. Accurate polynomial evaluation in floating point arithmetic. In *12th GAMM - IMACS International Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics, SCAN'06, Duisburg, Germany*, September 2006.

[78] P. Langlois and N. Louvet. Faithful horner algorithm. In SIAM, editor, *6th International Congress on Industrial and Applied Mathematics, Zurich, Switzerland*, page 252. Society for Industrial and Applied Mathematics, July 2007.

[79] P. Langlois and N. Louvet. Accurate solution of triangular linear system. In *13th GAMM - IMACS International Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics, El Paso (TX), USA*, September 2008.

[80] M. Martel. Towards an abstraction of the physical environment of embedded systems. In *Int. Workshop on Numerical and Symbolic Abstract Domains, NSAD'05*, 2005.

[81] D. Parello, M. Bouache, and B. Goossens. Improving multi/many core cycle-level simulation. In *Workshop on Massively Multiprocessor and Multicore Computers*, Rocquencourt, January 2009.

[82] B. Senouci, A. El Moussaoui, and B. Goossens. Software platform based embedded multiprocessor soc prototyping. In *Actes de la Conférence Internationale sur l'Informatique et ses Applications, Saida, Algérie*, 2009.

4.6 Communications par affiche dans des conférences (AFF)

[83] O. Bouissou and M. Martel. Static analysis of embedded programs with continuous i/o, 2007.

[84] A. Chapoutot and M. Martel. Abstract frequency analysis of synchronous systems, 2006.

[85] S. Graillat. Pseudozero set of multivariate polynomials. Poster, 8th International Workshop on Computer Algebra in Scientific Computing, Kalamata, Greece, September 12-16, 2005.

[86] P. Langlois and N. Louvet. Fast and extra precise substitution. In *CSC05 : Second International Workshop on Combinatorial Scientific Computing*. Toulouse, France, June 2005.

4.7 Autres publications (AP)

[87] J.-C. Bajard, L. Imbert, and C. Negre. Arithmetic operations in finite fields of medium prime characteristic using the lagrange representation. Technical Report 05028, LIRMM, October 2005.

[88] J.-C. Bajard, C. Negre, and T. Plantard. Double polynomial basis representation for binary field arithmetic. Technical Report 5, DALI, July 2005.

[89] S. Collange, Y. Dandass, M. Daumas, and D. Defour. Using graphics processors for parallelizing hash-based data carving. Technical report, HAL-CCSD, 2009.

[90] S. Collange, D. Defour, and D. Parello. Barra, a modular functional gpu simulator for gpgpu. Technical Report hal-00359342, HAL-CCSD, January 2009. Submitted to SAMOS'09.

[91] S. Graillat. Applications of fast and accurate summation in computational geometry. Research Report 03, Équipe de recherche DALI, Laboratoire LP2A, Université de Perpignan Via Domitia, France, 52 avenue Paul Alduy, 66860 Perpignan cedex, France, May 2005.

[92] S. Graillat. *Fiabilité des algorithmes numériques : pseudo-solutions struturées et précision*. Doctorat en informatique, Université de Perpignan Via Domitia, November 2005.

[93] S. Graillat. Structured condition number and backward error for eigenvalue problems. Research Report 01, Équipe de recherche DALI, Laboratoire LP2A, Université de Perpignan Via Domitia, France, 52 avenue Paul Alduy, 66860 Perpignan cedex, France, January 2005.

[94] S. Graillat. Pseudozero set of multivariate polynomials. Research Report 02, Équipe de recherche DALI, Laboratoire LP2A, Université de Perpignan Via Domitia, France, 52 avenue Paul Alduy, 66860 Perpignan cedex, France, February 2006.

[95] S. Graillat, P. Langlois, and N. Louvet. Compensated horner scheme. Research Report 4, DALI Research Team, Université de Perpignan, France, July 2005.

[96] P. Langlois and N. Louvet. More instruction level parallelism explains the actual efficiency of compensated algorithms. Technical Report hal-00165020, DALI Research Team, HAL-CCSD, July 2007. (Submitted to IEEE Trans. Computers. In revision).

[97] N. Louvet. *Algorithmes compensés en arithmétique flottante : précision, validation, performances*. Doctorat en informatique, Université de Perpignan Via Domitia, November 2007.

[98] C. Negre. Finite field arithmetic using quasi-normal basis. Technical Report 02, DALI, 2005.

[99] C. Negre and T. Plantard. Prime field multiplication in adapted modular number system using lagrange representation. Research Report ccsd-00079454, version 2, DALI, 2006.

[100] F. Tisseur and S. Graillat. Structured condition numbers and backward errors in scalar product spaces. Numerical Analysis Report No. 473, Manchester Centre for Computational Mathematics, Manchester, England, September 2005.