

Arnaud TISSERAND, né le 25.03.1971 à Bourg en Bresse, nationalité française, célibataire

Coordonnées personnelles : 13 rue J. Monod, 69007 Lyon

Emploi : Chargé de Recherche CNRS, LIRMM, CNRS–Univ. Montpellier 2

Coordonnées professionnelles : LIRMM, CNRS-UM2, 161 rue Ada, F-34392 Montpellier.

Émail : arnaud.tisserand@lirmm.fr

Web : <http://www.lirmm.fr/~tisseran/>

1 Formation

1994–1997 Doctorat en Informatique effectué au Laboratoire de l’Informatique du Parallélisme à l’École Normale Supérieure de Lyon, bourse MENRT. Thèse soutenue le 25 septembre 1997 devant L. Dadda (rapporteur), D. Etiemble (rapporteur), J.-M. Muller (directeur de thèse), M. Renaudin (examinateur) et Y. Robert (président). Titre : *Adéquation Arithmétique Architecture : problèmes et étude de cas.*

1993–1994 Diplôme d’Études Approfondies en Informatique Fondamentale de l’École Normale Supérieure de Lyon et de l’Université Claude Bernard Lyon I.

1992–1993 Maîtrise d’Informatique de l’Université Claude Bernard Lyon I.

1991–1992 Licence d’Informatique de l’Université Claude Bernard Lyon I.

1989–1991 Diplôme Universitaire de Technologie, spécialité Génie Mécanique et Productique de l’Université Claude Bernard Lyon I.

2 Expérience professionnelle

03.2007-04.2008 Responsable de l’équipe/projet ARITH du LIRMM (10 permanents et 5 doctorants au 01.01.2008).

2005–aujourd’hui Chargé de Recherche CNRS (première classe), dans l’équipe ARITH au LIRMM (recrutement au premier octobre 2005).

1999–2005 Chargé de Recherche INRIA dans le projet Arénaire (LIP, ENS Lyon).

- CR1 du 01.10.2001 au 30.09.2005.
- CR2 du 01.10.1999 au 30.09.2001.

1997–1999 Post-doctorat au Centre Suisse d’Électronique et de Microtechnique (CSEM) à Neuchâtel en Suisse, salarié privé en CDI.

- Direction d’une équipe de recherche de 4 personnes du 01.01.1999 au 30.09.1999.
- Ingénieur Recherche & Développement du 01.10.1997 au 31.12.1998. Travail dans les projets de recherche de base du secteur *Ultra-Low Power* de la division micro-électronique du CSEM.

1994–1997 Doctorant au LIP, boursier MENRT, enseignant vacataire à l’ENS Lyon et l’Université Claude Bernard Lyon I.

3 Recherche

3.1 Domaines de recherche

- arithmétique des ordinateurs matérielle et logicielle : représentations des nombres, algorithmique, implantations, validations. . .
- architecture des ordinateurs : processeurs généralistes et spécialisés, supports de calcul, architectures parallèles sur puce, SoC, systèmes embarqués. . .
- outils de conception de circuits : générateurs automatiques d’opérateurs de calcul, support pour la synthèse d’arithmétiques évoluées. . .

Domaines d'application : traitement du signal et des images, calcul scientifique, cryptographie, contrôle numérique...

3.2 Principaux travaux

- Opérateurs arithmétiques pour l'évaluation de fonctions
- Opérateurs arithmétiques pour la cryptographie : opérations et représentations de base.
- Opérateurs arithmétiques à basse consommation d'énergie : multiplieurs et diviseurs.
- Opérateurs arithmétiques asynchrones : addition, multiplication et division.
- Algorithmes pour l'évaluation des fonctions élémentaires.
- Méthodes de calcul à base de tables et d'additions pour l'approximation de fonctions.
- Algorithmes de division : par des constantes, en grande précision, à base de tables et de petites multiplications.
- Arithmétique en-ligne : opérations de base, fonctions algébriques et élémentaires, développement de support pour la synthèse VHDL, conception d'un FPGA en arithmétique en-ligne.
- Outils de conception : générateurs d'opérateurs arithmétiques, bibliothèques support.
- Arrondi correct des fonctions élémentaires.
- Système semi-logarithmique de représentation des nombres.
- Architectures parallèles mono-puce.
- Convertisseurs analogiques numériques rapides.

4 Encadrement

4.1 Thèses

José Lopes, étudiant Université Montpellier 2, bourse ANR de 3 ans débutée en octobre 2007. Sujet : *opérateurs arithmétiques reconfigurables*. Accréditation pour encadrer cette thèse seul. Thèse abandonnée en fin de première année, effectuée au LIRMM.

Julien Francq, ingénieur Polytech'Montpellier, bourse CEA de 3 ans débutée en octobre 2006 soutenance prévue début 2009. Sujet : *représentation et codage de l'information pour l'amélioration de la sécurité des circuits intégrés*. Thèse co-encadrée avec Jean-Baptiste Rigaud (École des Nîmes de St-Étienne) et effectuée au Centre Microélectronique de Provence à Gardanne.

Stéphane Simard, ingénieur de l'Université du Québec à Chicoutimi au Canada, bourse de 3 ans débutée en septembre 2005. Sujet : *système sur puce en arithmétique en ligne pour le contrôle vectorielle sans capteur*. Thèse co-encadrée avec Rachid Bugénane (encadrant principal) et effectuée au laboratoire ERMETIS à l'UQAC Chicoutimi Canada.

Romain Michard, ingénieur du Corps des Télécommunications, bourse (détachement INRIA) de 4 ans débutée en juillet 2004, soutenance prévue pour le premier semestre 2008. Sujet : *opérateurs arithmétiques pour la basse consommation d'énergie*. Accréditation pour encadrer cette thèse seul. Thèse effectuée au LIP, ENS Lyon.

Nicolas Veyrat-Charvillon, étudiant ENS Lyon, bourse MENRT de 3 ans débutée en septembre 2004 et soutenance en juin 2007. Sujet : *opérateurs arithmétiques pour des applications spécifiques*. Thèse co-encadrée administrativement par J.-M. Muller et effectuée au LIP, ENS Lyon.

Saurabh-Kumar Raina, étudiant Indien, bourse Région Rhône-Alpes de 3 ans et soutenue en septembre 2006. Sujet : *bibliothèque flottante pour processeurs entiers*. Thèse co-encadrée avec C.-P. Jeannerod (encadrant principal) et J.-M. Muller (encadrant administratif) et effectuée au LIP, ENS Lyon.

Nicolas Boullis, élève normalien ENS Lyon, allocation couplée. Sujet : *génération d'opérateurs de multiplication par des constantes*. Thèse abandonnée en début de 4ième année, co-encadrée administrativement par J.-M. Muller et effectuée au LIP, ENS Lyon.

Fabio Restrepo, étudiant de l'Université de Cali, Colombie, thèse EPFL numéro 2457, soutenue en 2001. Titre : *outils de programmation d'une machine parallèle réalisée sur un seul circuit intégré*. Thèse financée par le CSEM et effectuée au Laboratoire de Systèmes Logiques de l'EPFL. Encadrement partiel pour le CSEM en 1997–1999.

Martin Dimmler, étudiant de l'Université de Karlsruhe, Allemagne, thèse EPFL numéro 2050, soutenue en 1999. Titre : *Digital Control of Micro-Systems using On-Line Arithmetic*. Thèse financée par le CSEM et effectuée à l'Institut d'Automatique de l'EPFL. Encadrement partiel pour le CSEM en 1997–1999.

4.2 Stages de DEA

Nicolas Veyrat-Charvillon, étudiant ENS Lyon, février–juillet 2004. Stage effectué au LIP, ENS Lyon. Sujet : *algorithmes de multiplication pour circuits asynchrones*.

Nicolas Boullis, élève normalien, février–juillet 2001. Stage effectué au LIP, ENS Lyon. Sujet : *algorithmes de division pour circuits asynchrones*.

Rivo Randrianarivoni, étudiant ENS Lyon, mars–juillet 1997, co-encadrement avec J.-M. Muller. Stage effectué au LIP, ENS Lyon. Sujet : *bibliothèque de calcul de fonctions élémentaires en multi-précision*.

4.3 Autres encadrements

Florent Botella, étudiant 2ème année IUT Informatique de Montpellier, mars–mai 2007. Stage effectué au LIRMM. Sujet : *Bibliothèque arithmétique pour la cryptographie*.

Daria Tioc, étudiant Université Technique de Cluj-Napoca en Roumanie, mars–avril 2005. Stage effectué au LIP, ENS Lyon. Sujet : *Implantation FPGA de l'algorithme RSA*.

Zsolt Mathe, étudiant Université Technique de Cluj-Napoca en Roumanie, mars–avril 2005. Stage effectué au LIP, ENS Lyon. Sujet : *Implantation FPGA de l'algorithme RSA*.

Gaetan Leurent, élève École Polytechnique 2ème année, juin–août 2004. Stage effectué au LIP, ENS Lyon. Sujet : *Opérateurs matériels pour la cryptographie*.

Julien Robert, étudiant ENS Lyon 1ère année, juin–juillet 2004. Stage effectué au LIP, ENS Lyon. Sujet : *Implantation du produit modulaire sur FPGA*.

Guillaume Duveau, élève École Polytechnique 2ème année, avril–juillet 2003. Stage effectué au LIP, ENS Lyon. Sujet : *implémentation FPGA d'un algorithme de signature par code correcteur d'erreurs*.

Guillaume Melquiond, élève normalien 1ère année, mai–juin 2001. Stage effectué au LIP, ENS Lyon. Sujet : *bibliothèque flottante efficace en VHDL synthétisable pour FPGA*.

5 Participations à des jurys

Participation à 2 jurys de thèse dont 2 fois en tant que rapporteurs.

- Invité sur la thèse de Robin Perrot en 2007 à l'Université Montpellier 2.
- Examineur sur la thèse de Florent Bernard en 2007 à l'Université Paris 8.
- Rapporteur sur la thèse de Jean-Luc Beuchat en 2001 à l'EPFL.
- Rapporteur sur la thèse d'Eméka Mosanya en 1998 à l'EPFL.

6 Brevet

Dépôt en janvier 1999, avec P. Marchal et C. Pigué, d'un brevet sur les *réseaux programmables d'opérateurs arithmétiques en-ligne*. Brevet appartenant au CSEM, domaine de validité : Suisse, Europe, États-unis.

7 Collaborations académiques

7.1 Nationales

ANR Architecture du Futur, 2007–2009 : Responsable local du projet baptisé ROMA *Reconfigurable Operators for Multimedia Applications*. Travail commun avec l'IRISA (7 pers.), le CEA LIST (2 pers.), Thomson (2 pers.) et le LIRMM (2 pers.).

LIRMM, 2002–2005 : Travail commun avec J.-C. Bajard, L. Imbert, M. Robert et L. Torres sur des aspects arithmétique matérielle pour la cryptographie. En particulier nous travaillons sur les représentations des nombres (corps finis, représentation modulaire) et les opérateurs arithmétiques utilisées dans les algorithmes cryptographiques.

ACI Nouvelles Interfaces des Mathématiques, 2004–2007 : Responsable local du projet baptisé GAAP *Génération Automatique d'Approximants Polynomiaux* efficaces en machine. Travail commun avec le laboratoire LArAL de l'Université de St-Étienne. Étude et développement d'algorithmes et d'une bibliothèque pour la génération automatique d'approximations polynomiales de fonctions avec des contraintes sur les coefficients. Effectifs : 4 personnes à Lyon et 2 à St-Étienne. Site web : <http://lipforge.ens-lyon.fr/www/meplib/gaap/>

ACI Sécurité Informatique, 2003–2006 : Responsable local du projet baptisé OCAM *Opérateurs Cryptographiques et Arithmétique Matérielle* avec le projet INRIA CODES à (coord. N. Sendrier) et l'équipe Arithmétique Informatique du LIRMM à Montpellier (coord. J.-C. Bajard). Étude et implantation matérielle de primitives cryptographiques utilisant la théorie algébrique des codes. Implantation d'un prototype de système de signature numérique à sécurité élevée avec des signatures courtes. Effectifs : 5 personnes à Lyon, 3 à Rocquencourt et 2 à Montpellier. Site web : <http://www-rocq.inria.fr/codes/OCAM/>

ACI Cryptologie, 2002–2005 : Responsable local du projet baptisé OpAC *Opérateurs Arithmétiques pour la Cryptographie*. C'est un projet joint avec des membres des laboratoires LIRMM (départements informatique et micro-électronique, coord. J.-C. Bajard) et GTA (coord. P. Elbaz-Vincent) de Montpellier, travaillant dans divers domaines (géométrie arithmétique, théorie des nombres, calcul symbolique, arithmétique des ordinateurs, micro-électronique, architectures des ordinateurs, algorithmique). Effectifs : 3 à Lyon et 11 à Montpellier (7 LIRMM et 4 GTA). Site web : http://www.lirmm.fr/\protect\unhbox\voidb@x\penalty\M\bajard/ACI_CRYPTO/

ACI Jeunes Chercheurs, 2000–2003 : Action commune avec F. de Dinechin sur l'*arithmétique pour circuits FPGA*. Travaux sur les méthodes d'approximation de fonctions à base de tables et d'additions, l'arithmétique en-ligne, les opérations en virgule flottante et en système logarithmique. Acquisition d'un serveur, d'outils de CAO et de cartes FPGA.

CNET, 1995–1997 : Collaboration avec l'équipe de M. Renaudin du Centre National d'Études des Télécommunications sur la conception d'opérateurs arithmétiques asynchrones. Travail commun sur des additionneurs rapides asynchrones.

Participation à l'AS STIC *arithmétiques des ordinateurs* du CNRS créée en 2002 regroupant Arénaire, LIP6, LORIA, LIAFA, LIRMM, MANO Univ. Perpignan et LASTI ENSSAT Lannion. Travail sur l'arithmétique en virgule fixe.

Participations multiples aux journées Arinews : réunions de la communauté nationale en arithmétique des ordinateurs 1 à 2 fois par an.

7.2 Internationales

Université de Cork, Irlande, 2006, 2007 et 2008 : Collaboration avec le groupe de recherche sur les codes et la cryptographie. Bourse EGIDE PAI Ulysses en 2006, 2007 et 2008 pour financer des séjours de 2 semaines dans chaque sens. Travail commun sur l'étude et la conception d'opérateurs arithmétiques sur les courbes elliptiques et résistants à l'analyse simple de consommation.

Université du Québec à Chicoutimi, Canada, 2005-2007 : Collaboration avec le laboratoire ER-METIS (groupe de recherche en microélectronique et en traitement numérique du signal). Séjour en juillet 2006. Travail commun sur les opérateurs arithmétiques en-ligne pour le contrôle numérique.

University of California at Davis, U.S.A., 2005 : Collaboration avec le laboratoire Advanced Computer Engineering. Invitation de 15 jours sur le thème des opérateurs arithmétiques pour la basse consommation d'énergie.

Université de Calgary, Canada, 2004–2005 : Collaboration avec le laboratoire ATIPS dans l'équipe de G. Julien. Séjour en novembre 2004. Travail commun sur des opérateurs arithmétiques pour la cryptographie.

Université de Cardiff, Pays de Galles, 2001–2002 : Coordinateur français d'une action intégrée dans le cadre du programme franco-britannique Alliance avec l'équipe de N. Burgess. Séjour en 2001. Travail commun sur l'implantation FPGA du système logarithmique et d'opérateurs arithmétiques à basse consommation d'énergie. Accueils réciproques d'étudiants.

University of California at Los Angeles, U.S.A., 1995–aujourd'hui : Séjour de 1 mois, en février 2000, dans l'équipe de M. Ercegovac. Petits séjours en 1995, 1997, 2001, 2003 et 2004. Travail commun sur des opérateurs de division en très grande base, l'arithmétique en-ligne, l'évaluation des fonctions algébriques et élémentaires, les méthodes à base de tables et de petites multiplications. Cette collaboration a été financée par un projet PICS en 1997–1999.

University of California at Irvine, U.S.A., 2000 : Séjour d'un mois, en mars 2000, dans l'équipe de T. Lang. Travail commun sur ses opérateurs de division en très grande base et méthodes à base de petites multiplications et des tables.

EPFL, Lausanne, Suisse, 1997–1999 : Collaboration avec le Laboratoire de Systèmes Logiques et l'Institut d'Automatique. Travail commun sur l'arithmétique en-ligne et les systèmes parallèles mono-puce. Co-encadrement de thèses et des stages.

CSEM, Neuchâtel, Suisse, 1997–1999 : Post-doctorat au Centre Suisse d'Électronique et de Microtechnique à Neuchâtel en Suisse entre octobre 1997 et septembre 1999. Embauche sur un poste d'ingénieur de recherche et développement avec un contrat à durée indéterminée. Passage au grade de chef d'équipe de recherche en janvier 1999 (équipe de 4 personnes). Travaux communs et personnels sur les opérateurs arithmétiques pour la basse consommation, les circuits asynchrones, les réseaux de processeurs massivement parallèles mono-puce et des plate-formes de traitement d'image. Réalisation de blocs de calcul pour plusieurs circuits industriels. Développement de bibliothèques de calcul scientifique pour les architectures parallèles mono-puce.

École d'Ingénieur de l'État de Vaud, Yverdon, Suisse, 1997–1998 : Collaboration avec l'équipe de B. Hochet sur la conception de convertisseurs analogique/numérique de type *flash* pour l'instrumentation à très hautes performances (circuit AsGa).

Queen's University of Belfast, Irlande, 1995–1996 : Séjours dans l'équipe de J. Mc Canny et R. Woods. Travail commun sur l'utilisation de l'arithmétique en-ligne dans des algorithmes de traitement du signal et en particulier sur des applications de filtrage pour des disques durs.

8 Collaborations et contrats industriels

BEA Technologies, 2008 : Contrat dans le cadre de l'incubation de la société BEA Technologies par Languedoc Roussillon Incubation sur l'implantation matérielle d'algorithmes de chiffrement par flot.

STMicroelectronics, 2003–2006 : Contrat avec STMicroelectronics à Grenoble. Étude et implantation d'une bibliothèque flottante (opérations et fonctions élémentaires) pour la famille de processeurs entiers VLIW ST200. Travail commun avec C.-P. Jeannerod, J.-M. Muller et S. K. Raina.

STMicroelectronics, 2002 : Collaboration avec STMicroelectronics à Crolles sur l'étude et le développement d'une unité de calcul de multiplication/addition asynchrone pour le processeur ST20.

POSIC, 2001–2002 : Contrat INRIA avec POSIC S.A. à Neuchâtel en Suisse. Étude et implantation d'algorithmes et d'architectures de calcul rapide pour les capteurs de position. Participation à la réalisation d'un logiciel de test et d'une carte prototype FPGA.

STMicroelectronics, 2000–2001 : Contrat INRIA avec STMicroelectronics à Montbonnot. Sujet : algorithmes de division par des constantes pour le processeur DSP ST100. Travail commun avec J.-M. Muller et implanté dans la version de juin 2001 du compilateur vendu par STMicroelectronics.

- CSEM, 2000** : Contrat INRIA avec le Centre Suisse d'Électronique et de Microtechnique à Neuchâtel en Suisse. Étude et développement de blocs de calcul spécifiques pour le traitement d'image pour un prototype à base de FPGA et un circuit ASIC.
- Intel, 1996** : Participation au *P6 User Test Program* d'Intel. Don d'une machine à base du processeur *Pentium Pro* (P6) pour en tester l'arithmétique. Travail commun avec J.-M. Muller.
- CSEM, 1996** : Séjour de 6 semaines dans le groupe aérospatial du Centre Suisse d'Électronique et de Microtechnique à Neuchâtel en Suisse sur l'implantation FPGA d'opérateurs *en-ligne* pour des applications de contrôle numérique embarqués dans les satellites.
- DIGITAL, 1994–1995** : Contrat EERP avec la société DIGITAL sur l'implantation d'arithmétiques *en-ligne* sur la carte DECPeRLe-1, carte composées de 23 circuits FPGA Xilinx XC 3090. Travail commun avec M. Daumas et J.-M. Muller.

9 Logiciels

- **PACE**, *Prototyping Arithmetic in Cryptography Easily* :
Bibliothèque C++ modulaire et haute performance pour la représentation des nombres et les calculs en cryptographie.
Développement commun avec P. Giorgi, L. Imbert et A. Perreira.
- **Seedgen**, *générateur d'approximations rapides pour l'inverse et la racine carrée inverse en matériel* :
Programme C, sous licence GPL, pour la génération automatique d'opérateurs matériels pour l'approximation rapide de l'inverse et la racine carrée inverse.
L'algorithme utilisé dans ce programme est issu d'une collaboration avec M. Ercegovac (UCLA) et J.-M. Muller (LIP).
Site web : <http://www.lirmm.fr/~tisseran/devel/seedgen/>
- **MEPLib**, *machine-efficient polynomial library* :
Bibliothèque C, sous licence LGPL, pour la génération automatique d'approximations polynomiales de fonctions avec des contraintes sur les coefficients : formats des coefficients, valeurs ou domaines de valeurs.
Développement commun avec N. Brisebarre, F. Hennecart, J.-M. Muller et S. Torres dans le cadre de l'ACI *nouvelles interfaces des mathématiques*.
Site web : <http://lipforge.ens-lyon.fr/projects/meplib/>
- **Divgen**, un générateur de diviseurs matériels :
Programme, distribué sous licence GPL, de génération de descriptions VHDL synthétisables et optimisées d'opérateurs de division. Paramètres : type d'algorithme, base, type de représentation intermédiaire, optimisations au niveau architectural/circuit, circuits cibles ASIC ou FPGA.
Développement commun avec R. Michard et N. Veyrat-Charvillon.
Ce programme a été utilisé dans le cadre d'une collaboration entre le CEA-Léti et l'INRIA.
Site web : <http://lipforge.ens-lyon.fr/projects/divgen/>
- **FLIP**, *floating-point library for integer processor* :
Bibliothèque C de support pour le calcul flottant sur des processeurs entiers ou en virgule fixe (i.e. sans unité flottante). Les différentes opérations de base sont implantées et optimisées pour la simple précision et la famille de processeurs VLIW ST200 de STMicroelectronics.
Développement commun avec C.-P. Jeannerod, J.-M. Muller et S. K. Raina.
Cette bibliothèque est développée dans le cadre d'une collaboration avec la société STMicroelectronics à Grenoble et fait l'objet d'un support financier de la région Rhône-Alpes (bourse de thèse de S. K. Raina).
- Bibliothèque VHDL synthétisable d'arithmétique en-ligne pour FPGA :
Opérateurs de calcul en arithmétique en-ligne, types de données, opérateurs de conversion. Cette bibliothèque a été utilisée à l'ENS Lyon, l'EPFL, au CSEM et au LORIA.

10 Enseignement

- 2003–2005** : Cours de *circuits intégrés numériques* dans le master recherche (DEA en 2003–2004) 2ème année, spécialité Informatique Fondamentale, à l'ENS Lyon. Durée : 30 h par an, effectif : environ

10 étudiants chaque année.

2001–2002 : Cours de *conception d'architectures matérielles* dans le DEA d'Informatique de l'ENS Lyon. Cours commun avec F. de Dinechin. Durée par personne : 12 h par an, effectif : environ 10 étudiants chaque année.

1997–1999 : Formateur interne au CSEM sur les outils Unix, administration système Solaris et l'environnement de programmation C/C++.

1996–1997 : Cours et TD de *circuits Intégrés* en 1ère année du Magistère d'Informatique de l'École Normale Supérieure de Lyon (2ème cycle). Durée : cours 14 h et TD 28 h, effectif : 20 étudiants.

TD en *programmation informatique* en 1ère année du Magistère d'Informatique et du Magistère de Mathématiques de l'École Normale Supérieure de Lyon. Durée : 28 h, effectif : 20 étudiants.

Formation continue au logiciel *Maple* des enseignants/chercheurs du LIP. Durée : 8 h, effectif : 10 personnes.

1995–1996 : Cours et TD de *circuits intégrés* en 1ère année du Magistère d'Informatique de l'École Normale Supérieure de Lyon. Durée : cours 14 h et TD 14 h, effectif : 20 étudiants.

TD d'*informatique* en DEUG MASS 1ère année de l'Université Claude Bernard Lyon I. Durée : 20 h, effectif : 40 étudiants.

TD en *programmation informatique* en 1ère année du Magistère d'Informatique et du Magistère de Mathématiques de l'École Normale Supérieure de Lyon. Durée : 28 h, effectif : 25 étudiants.

Formation continue au logiciel *Maple* des professeurs des lycées du Parc et Jean Perrin de Lyon. Durée : 24 h, effectif : 12 personnes.

Interrogateur oral en informatique Math Spé M' et HEC au Lycée du Parc de Lyon.

1994–1995 : TD de *circuits intégrés* en 1ère année du Magistère d'Informatique de l'École Normale Supérieure de Lyon. Durée : 14 h, effectif : 25 étudiants.

TP d'*informatique* en DEUG MASS 1ère de l'Université Claude Bernard Lyon I. Durée : 50 h, effectif : 40 étudiants.

Interrogateur oral en informatique Math Spé M' au Lycée du Parc de Lyon.

Formation continue pour SUN Microsystems en 1995–1997 et 1999–2001. Formations « Unix », « installation et administration système », et « administration système avancée ». Environ 10 formations au total d'une semaine et de 6 à 8 personnes.

11 Participation aux tâches collectives

Responsable de l'équipe/projet ARITH, 2007–2008 : équipe de 10 permanents et 5 doctorants au 01.01.2008. Site web de l'équipe : <http://www.lirmm.fr/arith/>.

Représentant CURI, 2005–2007 : représentant du département informatique du LIRMM à la CURI.

Administration serveurs et outils CAO au LIP, 1999–aujourd'hui : Gestion, installation et maintenance des serveurs (4 machines sur 2 OS) et des outils (environ 12) pour la CAO de circuit VLSI et FPGA au LIP. Environ 15 utilisateurs sur deux équipes.

Membre comité scientifique écoles thématiques d'architecture, depuis 2002 : écoles thématiques du CNRS *Architectures des systèmes matériels enfouis et méthodes de conception associées*.

Responsable moyens informatiques LIP, 2001–2003 : Direction équipe de 3 ingénieurs. Administration système des machines et outils logiciels du LIP (50 machines et 100 utilisateurs environ).

Président commission informatique LIP, 2000–2003.

Organisateur séminaires LIP, 1999–2000 : 2 fois par mois.

Chef de projet, CSEM, 1999 : Organisation et administration d'un projet de recherche de base du CSEM (préparation et animation des réunions, valorisation, contacts industriels, rapport internes...). Équipe de 4 personnes.

Administration système et outils informatiques, CSEM, 1997–1997 : Mise en œuvre et maintenance d'applications informatiques (compilateurs, bibliothèques graphiques, outils de calcul numérique et symbolique, éditeurs...).

Animation Réseau Doctoral AMS, 1995–1997 : pour le pôle lyonnais du Réseau Doctoral en Architectures de Machines et Systèmes.

Webmaster LIP, 1995–1997 : Mise en place et maintenance du serveur WEB du LIP.

12 Organisation de rencontres

Co-organisateur ARCHIO9, Pleumeur-Bodou, mars 2009 : 5ème école thématique *Architectures des systèmes matériels enfouis et méthodes de conception associées* (<http://www.irisa.fr/archi09/>). Co-organisation avec O. Sentieys et S. Pillement.

Co-organisateur ARITH18, Montpellier, juin 2007 : *18th IEEE Symposium on Computer Arithmetic* (<http://www.lirmm.fr/arith18/>). Co-organisation avec L. Imbert.

Co-organisateur ARCHIO7, Boussens, mars 2007 : 4ème école thématique *Architectures des systèmes matériels enfouis et méthodes de conception associées* (<http://www.lirmm.fr/archi07/>). Co-organisation avec C. Rochange.

Organisateur ARCHIO5, Autrans, mars 2005 : 3ème école thématique *Architectures des systèmes matériels enfouis et méthodes de conception associées* (<http://www.ens-lyon.fr/ARCHIO5/>).

Co-organisateur ARCHIO3, Roscoff, octobre 2002 : 2ème école thématique *Architectures des systèmes matériels enfouis et méthodes de conception associées* (<http://www.irisa.fr/archi03/>). Co-organisation avec F. Charot et O. Sentieys.

Co-organisateur *Real Numbers and Computers*, Saint-Étienne, avril 1995 : conférence co-organisée avec M. Daumas, A. Mignotte et J.-M. Muller.

Co-organisateur JJCAMS, Monastir, Tunisie, décembre 1994. Journées des Jeunes Chercheurs en Architecture de Machines et Systèmes.

13 Édition, comités de programmes

2008–aujourd’hui : Membre du comité de programme des conférences : *IEEE Symposium on Computer Arithmetic* (ARITH19), Faible Tension Faible Consommation (FTFC), Symposium d’architecture des machines (SympA).

2006–aujourd’hui : éditeur associé de la revue *International Journal of High Performance Systems Architecture* (<http://www.inderscience.com/ijhpsa>).

2001 : Co-édition avec M. Daumas et F. de Dinechin d’un numéro spécial de la revue Réseaux Systèmes Répartis, Calculateurs Parallèles sur l’*arithmétique des ordinateurs*. Vol. 13, n° 4-5. 2001. Introduction de 29 pages et 7 chapitres invités soit un total de 200 pages environ.

1999–2004 : Multiples participations aux visites organisées et aux présentations de la fête de la science à l’ENS Lyon.

1997 : Membre du comité de programme SCAN 97 *GAMM/IMACS International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics*, en septembre à Lyon.

1994 : Membre comité de programme des Journées des Jeunes Chercheurs en Architecture de Machines et Systèmes, en décembre à Monastir, Tunisie. Responsable de la session *technologies programmables*.

Participation à la relecture d’articles pour différents journaux : IEEE Transactions on Computers, IEEE Transactions on Circuits and Systems, IEEE Transactions on VLSI Systems, IEEE Journal on Solid State Circuits, IEEE Design and Test, IEEE Transactions on Parallel and Distributed Systems, Journal of VLSI Signal Processing, ACM Transactions on Embedded Computing Systems, ACM Transactions on Design Automation of Electronic Systems, International Journal of High Performance Systems Architecture, Integration the VLSI Journal, Computer Journal, Electronic Letters, Journal of Systems Architecture, IET Circuits Devices & Systems, Techniques et Science Informatique, Microelectronics Journal, ASP Journal of Low Power Electronics.

Participation à la relecture d’articles pour différentes conférences : ARITH, FPL, ASAP, PATMOS, ISPLED, ICCS, ISSAC, ISCAS, DATE, SAC, ReConfig, DDECS, SYMPA, FTFC, FPT, RNC, SCAN, ICES, IWLAS, WAIFI, STACS.

14 Commissions de spécialistes

Membre extérieur de la commission de spécialistes de l'Université du Sud, Toulon-Var, 27ème section, 2007–aujourd'hui.

Membre extérieur de la commission de spécialistes de l'Université Joseph Fourier à Grenoble, 27ème section, 2003–2004.

15 Divers

Langues étrangères : anglais courant (lu, parlé, écrit), espagnol débutant.

Permis de conduire : auto.

16 Publications et exposés/séminaires

Mises à jour régulières et accès en-ligne à certaines publications :

<http://www.lirmm.fr/~tisseran/publications/>

Chapitres de livres

- [1] A. Tisserand. Low-power arithmetic operators. In C. Piguët, editor, *Low Power Electronics Design*, chapter 9. CRC Press, November 2004. 1
- [2] J.-L. Beuchat and A. Tisserand. Opérateurs arithmétiques pour FPGA. In J.-C. Bajard and J.-M. Muller, editors, *Arithmétique des ordinateurs*, Traité I2C : Information–Commande–Communication, chapter 4, pages 109–152. Hermes, Lavoisier, 2004. 2
- [3] M. Daumas, F. de Dinechin, and A. Tisserand. Introduction au numéro spécial sur l'arithmétique des ordinateurs. In M. Daumas, F. de Dinechin, and A. Tisserand, editors, *L'arithmétique des ordinateurs*, volume 13 of *Réseaux et systèmes répartis, calculateurs parallèles*, pages 327–356. Hermes, December 2001. 3

Thèse et mémoires

- [4] A. Tisserand. *Adéquation Arithmétique Architecture : problèmes et études de cas*. Thèse de doctorat, Ecole Normale Supérieure de Lyon, Lyon, France, September 1997. 1
- [5] A. Tisserand. Arithmétique en-ligne sur l'accélérateur matériel DECPeRLe-1. Mémoire de stage de DEA, Ecole Normale Supérieure de Lyon, Lyon, France, June 1994. 2

Brevets

- [6] P. Marchal, A. Tisserand, and C. Piguët. Réseaux programmables d'opérateurs arithmétiques en-ligne. Brevet du Centre Suisse d'Electronique et de Microtechnique (CSEM), Neuchâtel, Switzerland, January 1999. Validity Domain : Switzerland, Europe, U.S.A. 1

Édition d'actes et numéros spéciaux

- [7] M. Daumas, F. de Dinechin, and A. Tisserand, editors. *L'arithmétique des ordinateurs*, volume 13 of *Réseaux et systèmes répartis, calculateurs parallèles*. Hermes, December 2001. 1
- [8] M. Daumas, A. Mignotte, J.-M. Muller, and A. Tisserand, editors. *IMACS-GAMM International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics*, Lyon, France, September 1997. 2

Articles de revues internationales

- [9] A. Byrne, N. Meloni, A. Tisserand, E. M. Popovici, and W. P. Marnane. Comparison of simple power analysis attack resistant algorithms for an elliptic curve cryptosystem. *Journal of Computers*, 2(10) :52–62, 2007. 1
- [10] A. Byrne, F. Crowe, W. P. Marnane, N. Meloni, A. Tisserand, and E. M. Popovici. SPA resistant elliptic curve cryptosystem using addition chains. *Int. J. High Performance Systems Architecture*, 1(2) :133–142, October 2007. 2
- [11] A. Tisserand. High-performance hardware operators for polynomial evaluation. *Int. J. High Performance Systems Architecture*, 1(1) :14–23, March 2007. invited paper. 3
- [12] R. Glabb, L. Imbert, G. Jullien, A. Tisserand, and N. Veyrat-Charvillon. Multi-mode operator for SHA-2 hash functions. *Journal of Systems Architecture*, 53(2-3) :127–138, February 2007. Special issue on "Embedded Hardware for Cryptosystems". 4
- [13] N. Brisebarre, J.-M. Muller, A. Tisserand, and S. Torres. Hardware operators for function evaluation using sparse-coefficient polynomials. *IEE Electronics Letters*, 42(25) :1441–1442, December 2006. 5
- [14] N. Brisebarre, J.-M. Muller, and A. Tisserand. Computing machine-efficient polynomial approximations. *ACM Transactions on Mathematical Software*, 32(2) :236–256, June 2006. 6
- [15] N. Boullis and A. Tisserand. Some optimizations of hardware multiplication by constant matrices. *IEEE Transactions on Computers*, 54(10) :1271–1282, October 2005. 7
- [16] F. de Dinechin and A. Tisserand. Multipartite table methods. *IEEE Transactions on Computers*, 54(3) :319–330, March 2005. 8
- [17] M. D. Ercegovic, T. Lang, J.-M. Muller, and A. Tisserand. Reciprocation, square root, inverse square root, and some elementary functions using small multipliers. *IEEE Transactions on Computers*, 49(7) :628–637, July 2000. 9
- [18] B. Girau and A. Tisserand. MLP computing and learning on FPGA using on-line arithmetic. *International Journal of Systems Research and Information Science*, 9(2–4), 1999. 10
- [19] M. Dimmler, A. Tisserand, U. Holmberg, and R. Longchamp. On-line arithmetic for real-time control of microsystems. *IEEE/ASME Transactions on Mechatronics*, 4(2) :213–217, June 1999. 11
- [20] V. Lefèvre, J.-M. Muller, and A. Tisserand. Toward correctly rounded transcendentals. *IEEE Transactions on Computers*, 47(11) :1235–1243, November 1998. 12
- [21] J.-M. Muller, A. Scherbyna, and A. Tisserand. Semi-logarithmic number systems. *IEEE Transactions on Computers*, 47(2) :145–151, February 1998. 13

Articles de revues nationales

- [22] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Optimisation d'opérateurs arithmétiques matériels à base d'approximations polynomiales. *Technique et Science Informatiques*, 2008. 1
- [23] A. Tisserand. Introduction aux représentations des nombres et opérateurs arithmétiques à basse consommation d'énergie. *Technique et Science Informatiques*, 26(5) :639–646, May 2007. 2
- [24] J.-L. Beuchat and A. Tisserand. Évaluation polynomiale en-ligne de fonctions élémentaires sur FPGA. *Technique et Science Informatiques*, 23(10) :1247–1267, 2004. 3

Invitations à des conférences

- [25] A. Tisserand. Algorithms and number systems for hardware computer arithmetic. In *International Symposium on Symbolic and Algebraic Computation (ISSAC)*, Beijing, China, July 2005. Invited tutorial. 1

Articles de conférences internationales

- [26] L. Imbert, A. Peirera, and A. Tisserand. A library for prototyping the computer arithmetic level in elliptic curve cryptography. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architectures and Implementations XVII*, volume 6697, pages 1–9, San Diego, California, U.S.A., August 2007. SPIE. 1
- [27] A. Tisserand. Hardware reciprocation using degree-3 polynomials but only 1 complete multiplication. In *Proc. 5th International Northeast Workshop on Circuits & Systems (NEWCAS)*, pages 301–304, Montréal, Canada, August 2007. IEEE. 2
- [28] A. Byrne, N. Meloni, F. Crowe, W. P. Marnane, A. Tisserand, and E. M. Popovici. SPA resistant elliptic curve cryptosystem using addition chains. In *Proc. 4th International Conference on Information Technology (ITNG)*, pages 995–1000, Las Vegas, Nevada, U.S.A., April 2007. IEEE. 3
- [29] A. Tisserand. Automatic generation of low-power circuits for the evaluation of polynomials. In *Proc. 40th Asilomar Conference on Signals, Systems and Computers*, pages 2053–2057, Pacific Grove, California, U.S.A., October 2006. IEEE. 4
- [30] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Carry prediction and selection for truncated multiplication. In *Workshop on Signal Processing Systems (SiPS)*, pages 339–344, Banff, Canada, October 2006. IEEE. 5
- [31] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. New identities and transformations for hardware power operators. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architectures and Implementations XVI*, volume 6313, pages 1–10, San Diego, California, U.S.A., August 2006. SPIE. 6
- [32] R. Beguenane, S. Simard, and A. Tisserand. Function evaluation on FPGAs using on-line arithmetic polynomial approximation. In *Proc. 4th International Northeast Workshop on Circuits and Systems (NEWCAS)*, pages 21–24, Gatineau, Canada, June 2006. IEEE. 7
- [33] R. Glabb, L. Imbert, G. Jullien, A. Tisserand, and N. Veyrat-Charvillon. Multi-mode operator for SHA-2 hash functions. In *Proc. International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA)*, pages 207–210, Las Vegas, Nevada, U.S.A., June 2006. 8
- [34] R. Beguenane, J.-G. Mailloux, S. Simard, and A. Tisserand. Towards the system-on-chip realization of a sensorless vector controller with microsecond-order computation time. In *Proc. Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 908–912, Ottawa, Canada, May 2006. IEEE. 9
- [35] A. Tisserand. Hardware operator for simultaneous sine and cosine evaluation. In *Proc. International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, volume 3, pages 992–995, Toulouse, France, May 2006. IEEE. 10
- [36] M. D. Ercegovic, J.-M. Muller, and A. Tisserand. Simple seed architectures for reciprocal and square root reciprocal. In *Proc. 39th Asilomar Conference on Signals, Systems and Computers*, pages 1167–1171, Pacific Grove, California, U.S.A., October 2005. IEEE. 11
- [37] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Divgen : a divider unit generator. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architectures and Implementations XV*, volume 5910, pages 1–12, San Diego, California, U.S.A., August 2005. SPIE. 12
- [38] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Small FPGA polynomial approximations with 3-bit coefficients and low-precision estimations of the powers of x . In S. Vassiliadis, N. Dimopoulos, and S. Rajopadhye, editors, *Proc. 16th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pages 334–339, Samos, Greece, July 2005. IEEE Computer Society. Best Paper Award. 13
- [39] C.-P. Jeannerod, S.-K. Raina, and A. Tisserand. High-radix floating-point division algorithms for embedded VLIW integer processors. In *Proc. 17th World Congress on Scientific Computation, Applied Mathematics and Simulation IMACS*, Paris, France, July 2005. 14
- [40] J.-M. Muller, A. Tisserand, B. Dupont de Dinechin, and C. Monat. Division by constant for the ST100 DSP microprocessor. In P. Montuschi and E. Schwarz, editors, *Proc. 17th Symposium on Computer Arithmetic (ARITH)*, pages 124–130, Cape Cod, MA., U.S.A., June 2005. IEEE Computer Society. 15

- [41] N. Brisebarre, J.-M. Muller, and A. Tisserand. Sparse-coefficient polynomial approximations for hardware implementations. In *Proc. 38th Asilomar Conference on Signals, Systems and Computers*, pages 532–535, Pacific Grove, California, U.S.A., November 2004. IEEE. 16
- [42] C. Bertin, N. Brisebarre, B. Dupont de Dinechin, C.-P. Jeannerod, C. Monat, J.-M. Muller, S. K. Raina, and A. Tisserand. A floating-point library for integer processors. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architectures and Implementations XIV*, volume 5559, pages 101–111, Denver, Colorado, U.S.A., August 2004. SPIE. 17
- [43] J.-L. Beuchat, L. Imbert, and A. Tisserand. Comparison of modular multipliers on FPGAs. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architectures and Implementations XIII*, volume 5205, pages 490–498, San Diego, California, U.S.A., August 2003. SPIE. 18
- [44] N. Boullis and A. Tisserand. Some optimizations of hardware multiplication by constant matrices. In J.-C. Bajard and M. Schulte, editors, *Proc. 16th Symposium on Computer Arithmetic (ARITH)*, pages 20–27, Santiago de Compostela, Spain, June 2003. IEEE Computer Society. 19
- [45] J.-L. Beuchat and A. Tisserand. Small multiplier-based multiplication and division operators for Virtex-II devices. In M. Glesner, P. Zipf, and M. Renovell, editors, *Proc. 12th International Conference on Field-Programmable Logic and Applications (FPL)*, volume 2438 of *LNCS*, pages 513–522, Montpellier, France, September 2002. Springer. 20
- [46] N. Boullis and A. Tisserand. On digit-recurrence division algorithms for self-timed circuits. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architecture and Implementations XI*, volume 4474, pages 115–125, San Diego, California, U.S.A., August 2001. SPIE. 21
- [47] F. de Dinechin and A. Tisserand. Some improvements on multipartite tables methods. In N. Burgess and L. Ciminiera, editors, *Proc. 15th Symposium on Computer Arithmetic (ARITH)*, pages 128–135, Vail, Colorado, U.S.A., June 2001. IEEE Computer Society. 22
- [48] F. de Dinechin and A. Tisserand. Table-based methods comparison for low-precision evaluation of the sine and cosine functions on FPGAs. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architectures, and Implementations X*, volume 4116, pages 226–234, San Diego, California, U.S.A., August 2000. SPIE. 23
- [49] A. Tisserand, P. Marchal, and C. Pigué. An on-line arithmetic based FPGA for low-power custom computing. In *Proc. 9th International Workshop on Field Programmable Logic and Applications (FPL)*, volume 1673 of *LNCS*, pages 264–273, London, England, September 1999. Springer. 24
- [50] A. Tisserand, P. Marchal, and C. Pigué. FPOP : Field programmable on-line operators. In F. T. Luk, editor, *Proc. Advanced Signal Processing Algorithms, Architectures and Implementations IX*, volume 3807, pages 31–42, Denver, Colorado, U.S.A., September 1999. SPIE. 25
- [51] B. Girau, P. Marchal, P. Nussbaum, A. Tisserand, and H. F. Restrepo. A massively parallel one-chip architecture : Towards evolvable array processing. In *Proc. International Conference on Microelectronics for Neural Networks and Fuzzy Systems (MicroNeuro)*, pages 187–193, Granada, Spain, April 1999. IEEE. 26
- [52] F. Kaess, R. Kanan, M. Declercq, A. Tisserand, J.-M. Muller, B. Hochet, and J.-M. Vincent. A fast encoding architecture for high-speed flash analog-to-digital converters. In *Proc. 2nd International Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, pages 237–243, Szczyrk, Poland, September 1998. IEEE. 27
- [53] F. Kaess, R. Kanan, M. Declercq, A. Tisserand, J.-M. Muller, B. Hochet, and J.-M. Vincent. Improving high-speed flash analog-to-digital converters accuracy using sum encoding. In *Proc. International Symposium On Scientific Computing, Computer Arithmetic and Validated Numerics (SCAN)*, Budapest, Hungary, September 1998. 28
- [54] P. Nussbaum, B. Girau, and A. Tisserand. Field programmable processor arrays. In M. Shipper, D. Mange, and A. Perez-Urbe, editors, *Proc. 2nd International Conference on Evolvable Systems (ICES) : from biology to hardware*, volume 1478 of *LNCS*, pages 311–322, Lausanne, Switzerland, September 1998. Springer. 29
- [55] M. D. Ercegovac, T. Lang, J.-M. Muller, and A. Tisserand. Reciprocation, square root, inverse square root, and some elementary functions using small multipliers. In F. T. Luk, editor, *Proc.* 30

- Advanced Signal Processing Algorithms, Architectures, and Implementations VIII*, volume 3461, pages 543–554, San Diego, California, U.S.A., June 1998. SPIE.
- [56] A. Tisserand and M. Dimmler. FPGA implementation of real-time digital controllers using on-line arithmetic. In *Proc. 7th International Workshop on Field Programmable Logic and Applications (FPL)*, volume LNCS-1304, pages 472–481, London, England, August 1997. Springer. 31
- [57] J.-M. Muller, A. Tisserand, and J.-M. Vincent. Asynchronous sub-logarithmic adders. In *Proc. Pacific Rim Conference on Communication, Computers and Signal Processing (PACRIM)*, volume 2, pages 515–518, Victoria, Canada, August 1997. IEEE. 32
- [58] V. Lefèvre, J.-M. Muller, and A. Tisserand. Towards correctly rounded transcendental. In T. Lang, J.-M. Muller, and N. Takagi, editors, *Proc. 13th Symposium on Computer Arithmetic (ARITH)*, pages 132–137, Asilomar, California, U.S.A., July 1997. IEEE Computer Society. 33
- [59] M. Daumas, J.-M. Muller, and A. Tisserand. Very high radix on-line arithmetic for accurate computations. In *Proc. 15th World Congress on Scientific Computation, Modelling and Applied Mathematics (IMACS)*, Berlin, Germany, August 1997. 34
- [60] A. Tisserand. FPGA implementation of on-line arithmetic operators for digital control. In *Proc. International Workshop on Logic and Architecture Synthesis (IWLAS)*, pages 115–122, Grenoble, France, December 1996. 35
- [61] M. Daumas, J.-M. Muller, and A. Tisserand. Theoretical support for standardized elementary functions. In *Proc. International Symposium on Modelling, Analysis and Simulation (IMACS)*, volume 2, pages 1133–1138, Lille, France, July 1996. IEEE-SMC. 36
- [62] B. Girau and A. Tisserand. On-line arithmetic based reprogrammable hardware implementation of multilayer perceptron back-propagation. In *Proc. 5th International Conference on Microelectronics for Neural Networks and Fuzzy Systems (MicroNeuro)*, pages 168–175, Lausanne, Switzerland, February 1996. IEEE Computer Society. 37
- [63] M. D. Ercegovic, J.-M. Muller, and A. Tisserand. FPGA implementation of polynomial evaluation algorithm. In J. Schewel, editor, *Proc. Field Programmable Gate Arrays for Fast Board Development and Reconfigurable Computing*, volume 2607, pages 177–188, Philadelphia, Pennsylvania, U.S.A., October 1995. SPIE. 38
- [64] J.-M. Muller and A. Tisserand. Towards exact rounding of the elementary functions. In *Proc. International Symposium On Scientific Computing, Computer Arithmetic and Validated Numerics (SCAN)*, volume 90, pages 59–71, Wuppertal, Germany, September 1995. 39
- [65] J.-M. Muller, A. Scherbyna, and A. Tisserand. Semi-logarithmic number systems. In S. Knowles and W. H. McAllister, editors, *Proc. 12th Symposium on Computer Arithmetic (ARITH)*, pages 201–207, Bath, England, July 1995. IEEE Computer Society. 40

Articles de conférences nationales

- [66] A. Tisserand. Estimation rapide de l'activité parasite pour l'optimisation des arbres de réduction de multiplieurs. In *6ième journées d'études Faible Tension Faible Consommation (FTFC)*, pages 127–130, Paris, France, May 2007. 1
- [67] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Optimisation d'opérateurs arithmétiques matériels à base d'approximations polynomiales. In *11ième SYMPosium en Architectures nouvelles de machines (SYMPA)*, pages 130–141, Perpignan, France, October 2006. 2
- [68] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Étude statistique de l'activité de la fonction de sélection dans l'algorithme de e-méthode. In *5ième journées d'études Faible Tension Faible Consommation (FTFC)*, pages 61–65, Paris, France, May 2005. 3
- [69] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Evaluation de polynômes et de fractions rationnelles sur FPGA avec des opérateurs à additions et décalages en grande base. In *10ième SYMPosium en Architectures nouvelles de machines (SYMPA)*, pages 85–96, Le Croisic, France, April 2005. 4

- [70] J.-L. Beuchat and A. Tisserand. Opérateur en-ligne sur FPGA pour l'implantation de quelques fonctions élémentaires. In *8ème SYMPosium en Architectures nouvelles de machines (SYMPA)*, pages 267–274, Hamamet, Tunisie, April 2002. 5
- [71] N. Boullis and A. Tisserand. Génération automatique d'architectures de calcul pour des opérations linéaires : application à l'IDCT sur FPGA. In *8ème SYMPosium en Architectures nouvelles de machines (SYMPA)*, pages 283–290, Hamamet, Tunisie, April 2002. 6
- [72] A. Tisserand. Etude d'un produit scalaire haute précision sur mémoire active programmable. In *Journées Jeunes Chercheurs en Architectures de Machines et Systèmes*, pages 211–220, Monastir, Tunisie, December 1994. PRC ANM, Réseau Doctoral en Architecture de Machines et Systèmes. 7

Rapports de recherche

- [73] M. D. Ercegovac, J.-M. Muller, and A. Tisserand. Simple seed architectures for reciprocal and square root reciprocal. Research Report RR2005-49, Laboratoire de l'Informatique du Parallélisme (LIP), October 2005. Also available as INRIA Research Report RR-5720. 1
- [74] C.-P. Jeannerod, S.-K. Raina, and A. Tisserand. High-radix floating-point division algorithms for embedded VLIW integer processors. Research Report RR2005-39, Laboratoire de l'Informatique du Parallélisme (LIP), September 2005. 2
- [75] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Étude statistique de l'activité de la fonction de sélection dans l'algorithme de e-méthode. Research Report RR2005-25, Laboratoire de l'Informatique du Parallélisme (LIP), February 2005. Also available as INRIA Research Report RR-5574. 3
- [76] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Small FPGA polynomial approximations with 3-bit coefficients and low-precision estimations of the powers of x . Research Report RR2005-08, Laboratoire de l'Informatique du Parallélisme (LIP), February 2005. Also available as INRIA Research Report RR-5503. 4
- [77] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Evaluation de polynômes et de fractions rationnelles sur FPGA avec des opérateurs à additions et décalages en grande base. Research Report RR2004-62, Laboratoire de l'Informatique du Parallélisme (LIP), December 2004. Also available as INRIA Research Report RR-5437. 5
- [78] J.-M. Muller, A. Tisserand, B. Dupont de Dinechin, and C. Monat. Division by constant for the ST100 DSP microprocessor. Research Report RR2004-45, Laboratoire de l'Informatique du Parallélisme (LIP), October 2004. Also available as INRIA Research Report RR-5340. 6
- [79] C. Bertin, N. Brisebarre, B. Dupont de Dinechin, C.-P. Jeannerod, C. Monat, J.-M. Muller, S. K. Raina, and A. Tisserand. A floating-point library for integer processors. Research Report RR2004-37, Laboratoire de l'Informatique du Parallélisme (LIP), July 2004. Also available as INRIA Research Report RR-5268. 7
- [80] J.-L. Beuchat, N. Sendrier, A. Tisserand, and G. Villard. FPGA implementation of a recently published signature scheme. Research Report RR2004-14, Laboratoire de l'Informatique du Parallélisme (LIP), March 2004. Also available as INRIA Research Report RR-5158. 8
- [81] J.-L. Beuchat and A. Tisserand. Evaluation polynomiale en-ligne de fonctions élémentaires sur FPGA. Research Report RR2002-33, Laboratoire de l'Informatique du Parallélisme (LIP), September 2002. Also available as INRIA Research Report RR-4557. 9
- [82] J.-L. Beuchat and A. Tisserand. Small multiplier-based multiplication and division operators for Virtex-II devices. Research Report RR2002-25, Laboratoire de l'Informatique du Parallélisme (LIP), September 2002. Also available as INRIA Research Report RR-4494. 10
- [83] N. Boullis and A. Tisserand. Génération automatique d'architectures de calcul pour des opérations linéaires : application à l'IDCT sur FPGA. Research Report RR2002-10, Laboratoire de l'Informatique du Parallélisme (LIP), March 2002. Also available as INRIA Research Report RR-4486. 11
- [84] N. Boullis and A. Tisserand. On digit-recurrence division algorithms for self-timed circuits. Research Report RR2001-27, Laboratoire de l'Informatique du Parallélisme (LIP), July 2001. Also available as INRIA Research Report RR-4221. 12

- [85] F. de Dinechin and A. Tisserand. Some improvements on multipartite table methods. Research Report RR2000-38, Laboratoire de l'Informatique du Parallélisme (LIP), November 2000. Also available as INRIA Research Report RR-4059. 13
- [86] V. Lefèvre, J.-M. Muller, and A. Tisserand. The table maker's dilemma. Research Report RR98-12, Laboratoire de l'Informatique du Parallélisme (LIP), February 1998. 14
- [87] M. D. Ercegovac, T. Lang, J.-M. Muller, and A. Tisserand. Reciprocation, square root, inverse square root, and some elementary functions using small multipliers. Research Report RR97-47, Laboratoire de l'Informatique du Parallélisme (LIP), November 1997. 15
- [88] J.-M. Muller, A. Tisserand, and J.-M. Vincent. Asynchronous sub-logarithmic adders. Research Report RR97-12, Laboratoire de l'Informatique du Parallélisme (LIP), May 1997. 16
- [89] B. Girau and A. Tisserand. On-line arithmetic based reprogrammable hardware implementation of multilayer perceptron back-propagation. Research Report RR96-14, Laboratoire de l'Informatique du Parallélisme (LIP), June 1996. 17
- [90] M. D. Ercegovac, J.-M. Muller, and A. Tisserand. FPGA implementation of polynomial evaluation algorithm. Research Report RR95-34, Laboratoire de l'Informatique du Parallélisme (LIP), November 1995. 18
- [91] J.-M. Muller and A. Tisserand. Towards exact rounding of the elementary functions. Research Report RR95-33, Laboratoire de l'Informatique du Parallélisme (LIP), November 1995. 19
- [92] J.-M. Muller, A. Scherbyna, and A. Tisserand. Semi-logarithmic number systems. Research Report RR95-04, Laboratoire de l'Informatique du Parallélisme (LIP), February 1995. 20

Logiciels

- [93] L. Imbert, A. Peirera, and A. Tisserand. PACE : Prototyping arithmetics for cryptography easily. LGPL software, 2007. 1
- [94] A. Tisserand. bibword : a minor Emacs mode for keywords in BibTeX files. GPL software, 2005–2006. 2
- [95] A. Tisserand. seedgen : a VHDL generator for reciprocal and inverse square root seeds. GPL software, 2005–2006. 3
- [96] R. Michard, A. Tisserand, and N. Veyrat-Charvillon. Divgen : a divider generator. GPL software, 2004–2005. 4
- [97] N. Brisebarre, F. Hennecart, J.-M. Muller, A. Tisserand, and S. Torres. MEPLib : Machine efficient polynomial library. LGPL software, 2004–2006. 5
- [98] C.-P. Jeannerod, S. K. Raina, and A. Tisserand. FLIP : Floating-point library for integer processor. LGPL software, 2003–2006. 6
- [99] A. Tisserand. On-line arithmetic library. software, 1994–1998. 7

Séminaires

- [100] A. Tisserand. Library for prototyping the computer arithmetic level in crypto applications. Invited seminar at the Centre for Applied Cryptographic Research (CACR), University of Waterloo, August 2007. 1
- [101] A. Tisserand. Computer arithmetic for cryptography in the ARITH group. Exposé invité Crypto'Puces, April 2007. 2
- [102] A. Tisserand. Number recoding and low-power consumption. Exposé invité journée basse consommation GDR ISIS, March 2007. 3
- [103] A. Tisserand. Automatic generation of hardware arithmetic operators : a small example. Séminaire invité au LIRMM, March 2005. 4
- [104] A. Tisserand. Introduction aux FPGA. Séminaire invité à l'Université de Perpignan, June 2004. 5

- [105] A. Tisserand. Conception d'opérateurs arithmétiques : aspects matériels. Séminaire invité à l'ENSTA, Paris, March 2004. 6
- [106] A. Tisserand. Introduction aux FPGA. Séminaire au Magister d'Informatique Fondamentale de l'ENS-Lyon, December 2003. 7
- [107] A. Tisserand. DSP : des processeurs dédiés pour le traitement numérique du signal. Séminaire LIP, Lyon, May 2003. 8
- [108] A. Tisserand. Basse consommation d'énergie et opérateurs arithmétiques. Séminaire au Magister d'Informatique Fondamentale de l'ENS-Lyon, February 2002. 9
- [109] A. Tisserand. Basse consommation d'énergie et opérateurs arithmétiques. Séminaire LIP, Lyon, May 2003. 10
- [110] A. Tisserand. Le temps dans les puces électroniques. Exposé, Fête de la Science, Lyon, October 2000. 11
- [111] A. Tisserand. évaluation de fonctions à base de tables et d'additions sur FPGA. Séminaire invité au Laboratoire de Systèmes Logiques, EPFL, Lausanne, Suisse, December 2000. 12
- [112] A. Tisserand. Unités arithmétiques dans les processeurs. Séminaire invité à l'Université de Blois, December 2000. 13

Cours dans des écoles ou workshops

- [113] A. Tisserand. Unités de calcul flottant. Cours École Thématique ARCHI07, March 2007. 1
- [114] A. Tisserand. Méthode du *logical effort*. Cours École Thématique ARCHI05, March 2005. 2
- [115] A. Tisserand. Arithmétique des ordinateurs. Cours École Doctorale de l'ENS-Lyon, May 2004. 3
- [116] A. Tisserand. Arithmétique des ordinateurs. Cours École Jeunes Chercheurs en Algorithmique et Calcul Formel, April 2004. 4
- [117] A. Tisserand. Introduction aux FPGA. Cours, réunion ACI Sécurité Informatique, projet OCAM, ENS-Lyon, September 2003. 5
- [118] A. Tisserand. Opérateurs arithmétiques matériels. Cours École thématique du CNRS ARCHI03 : Architectures des systèmes matériels enfouis et méthodes de conception associées, Roscoff, April 2003. 6
- [119] A. Tisserand. Opérateurs arithmétiques matériels. Cours École thématique du CNRS : adéquation arithmétique-algorithmes, Dijon, March 2003. 7
- [120] A. Tisserand. Introduction à VHDL et aux outils FPGA. Cours Action Spécifique CNRS : arithmétique des ordinateurs, Lyon, February 2003. 8