ARCHI 09

Pleumeur-Bodou
30 mars – 3 avril 2009

École thématique

Architectures des systèmes matériels enfouis et méthodes de conception associées

`http ://www.irisa.fr/archi09/`

Bilan

Table des matières

1 Bilan de la participation

Il y avait 51 inscrits à cette école thématique (dont 14 intervenants). 5 agents CNRS (3 ingénieurs, 1 chargé de recherche et 1 directeur de recherche) ont participé à cette école thématique. La liste complète des participants et intervenants est disponible sur le site web. Le tableau récapitulatif ci-dessous démontre le succès grandissant de cette école thématique.

édition	2000	2003	2005	2007	2009
nb. total de personnes	≈ 25	44	37	41	51
nb. cours	9	13	12	8	14
nb. posters	–	–	7	7	9

Laboratoires d'origine des participants :
- CEA-LIST (Gif-sur-Yvette)
- Centre de recherche Christian Huygens (Lorient)
- ELIAUS (Perpignan)
- ETIS (Cergy)
- GIPSA-Lab (Grenoble)
- G-SCOP (Grenoble)
- INRIA-Tsinghua University (Beijing, Chine)
- Institut Jean Lamour (Vandoeuvre les Nancy)
- IRISA (Rennes et Lannion)
- IMS (Grenoble)
- Lab-STICC (Lorient)
- LEAT (Nice)
- LIP (Lyon)

- LIP6 (Paris)
- LIRMM (Montpellier)
- LORIA (Vandoeuvre les Nancy)
- Observatoire de Haute-Provence (St Michel l'Observatoire)
- Supélec (Cesson-Sévigné)
- TIMA (Grenoble)
- VERIMAG (Grenoble)

2 Bilan des soutiens

La réussite de cette école doit beaucoup au soutien indéfectible à la fois des grandes instances nationales universitaires nationales (CNRS, INRIA) et locales (Université Rennes 1 et ENSSAT) mais aussi aux collectivité locales (LTA, CG22) qui nous ont permis de proposer des livres à tous les participants comme support de cours.

- CNRS : Centre National de la Recherche Scientifique (soutien financier et logistique)
- CG22 : Conseil Général des Côtes d'Armor (soutien financier)
- ENSSAT : École Nationale Supérieure des Sciences Appliquées et de Technologie (soutien logistique)
- GDR ARP : Groupement de Recherche Architecture, Systèmes, Réseaux (soutien financier)
- INRIA : Institut National de Recherche en Informatique et Automatique (soutien financier et logistique)
- IRISA : Institut de Recherche en Informatique et Systèmes Aléatoires (soutien financier et logistique)
- LTA : Lannion-Trégor Agglomération (soutien financier)
- Mairie de Plemeur-Bodou (soutien logistique)
- UR1 : Université Rennes 1 (soutien financier et logistique)

Les aspects financiers sont présentés à la section 5.

3 Bilan scientifique

Cours

14 cours ont été donnés par 14 intervenants. Le total représente un volume de 24 heures de cours réparties sur 7 demi-journées. L'ensemble des supports de cours papier distribués aux participants représente un total de plus 1150 transparents. Tous ces supports de cours et le planning sont disponibles sur le site web de l'école.

- **Architectures et tendances des FPGA** par Lilian Bossuet
  Définition, reconfigurable, alternative aux ASIC, évolution des technologies, considérations économiques, les fabricants, domaines d'applications, évolution des prix, compromis flexibilité/performance, coût des jeux de masques, cycle de conception, comparaion avec des DSP, technologies de configuration, antifusible, NVCM, flash, SRAM, run-time, architectures des FPGA, matrices de connexions, topologie de routage, réseau de routage, architecture hiérarchique, éléments logiques configurables, logique à multiplexeurs, LUT, éléments de mémoire configurables, architecture mémoire, opérateurs arithmétiques embarqués, coeurs de processeurs, réseau d'horloge, consommation d'énergie, embarquer un FPGA dans un SoC, temps de configuration, configuration multi-contexte, reconfiguration partielle, reconfiguration dynamique, reconfiguration et OS, sécurisation des configurations, bibliographie.

- **Challenges in Full System Simulation** par Vania Joloboff
  Systèmes embarqués, objectifs industriels, conception dirigée par les modèles, types de simulation, simulation de systèmes complets (matériel et logiciel), accélération de la simulation, niveaux d'abtraction, compromis précision et vitesse, aspects normalisation, normes pour l'intéropérabilité, rappels SystemC, threads et ordonnancement, interface de communication, modèle transactionnel, connectivité, transaction bloquante ou non bloquante, annotation temporelle, simulateur FORMES, simulation de jeux d'instruction, traduction statique, traduction dynamique (cache), SimSoC, évaluation partielle, générer la sémantique des fonctions, précompilation, simulation des unités de gestion d'adresse, simulation multicoeur, traduction parallèle.
- **Compteurs de performances matériels** par Bernard Goossens
  Organes matériels de gestion du temps, horloge temps réel, ICH, RTC, compteur de temps HPET, HZ, Jiffy, compteurs de temps locaux, APIC, interruption du HPET, dates systèmes, mesure de temps écoulé, datation des événements, aspects temporels des processus, appels systèmes, mesure de temps d'exécution (effectif), TSC, micro-architecture, problèmes de sérialisation, ordonnancement des instructions de mesure, perturbation des mesures, RDTSCP, mesure de latence, exemples q6600 et xeon 5410, exemple addition vectorielle, compteurs de performance matriels, registres MSR, lecture des registres, modules noyau, exécution pipelinée, exemples de mesures.
- **Cryptographie matérielle** par Guy Gogniat
  Contexte et enjeux, attaques d'un système embarqué communicant, attaques et protections, pyramide de sécurité, vocabulaire, principe de Kerckhoff, modèle de sécurité, principe de chiffrement, algorithmes symétriques, algorithmes asymétriques, chiffrement par bloc, chiffrement par flot, clé privée, clé publique, fonction à sens unique, fonction de hachage, MAC, distribution de clés, signature numérique, authentification, systèmes classiques de chiffrement, algorithme DES, permutations, rondes, génération de clés, algorithme triple DES, pipeline, coeurs IP, algorithme AES, NIST, cryptographie sur FPGA, dictionnaire de codes, enchainement des blocs, chiffrement à rétroaction, cryptographie à clé publique, fonction à trappes à sens unique, Diffie-Hellman, RSA, square and multiply, algorithme de Montgomery, cryptographie sur les courbres elliptiques, ECDH, addition de points, doublement de points, hachage MD5, hachage SHA, SHA2, SHA3, cryptographie quantique.
- **Evolution des technologies d'interconnexions : impacts pour la conception architecturale** par Olivier Sentieys
  Systèmes sur puces, challenges dans les interconnexions, évolution technologique, baisse des tensions d'alimentation, éléments parasites, longueurs des interconnexions, réduction des délais, modèles de délai, couplage capacitif, temps de propagation, coût des circuits, puissance et énergie, variations du processus de fabrication, erreurs, bruits, rapport délais porte et interconnexions, *scaling*, longueurs des interconnexions, modèles de délai, *cross-talk*, modèles de bruits, diminuer l'activité, codage de bus, lien ternaire, nombre variable de cycles, codes correcteurs d'erreurs, interconnexion CDMA, optimisation des canaux de communication, schéma de codage unifié, bibliographie
- **Exploitation du parallélisme et de la taille des données dans la conception d'opérateurs** par Emmanuel Casseau
  Ressources classiques de calcul, SWP subword parallelism, parallélisme interne aux données, exemples de parallélisme interne, applications, SWP orienté calcul, primitives SWP, impacte sur le codage de boucle, extension mutlimédia pour les processeurs de calcul généraliste, jeu d'instruction MAX2, arithmétique à saturation, SWP dans les processeurs de traitement du signal DSP, conception d'opérateurs SWP, addition, partitionnement d'opérateurs,

carry look ahead, multiplication, recodage de Booth, opérateur SWP reconfigurable, consommation d'énergie, références.

- **Gestion système de la consommation énergétique dans un SoC : systèmes monoprocesseur et multiprocesseur** par Cécile Belleudy
  Système basse consommation, contraintes énergétiques, ordonnancement temps réel, politiques d'ordonnancement, ordonnancement basse consommation, voltage and frequency scaling, VFS, DVFS, WCET, préemption, batteries, modèles de consommation, exemple ARM 1176, modes repos des processeurs, consommation mémoire, architecture mémoire multibanc, allocation optimisée, modèle mémoire, composantes de l'énergie, caractérisation des tâches, techniques de VFS, ordonnancement et DVFS, gestion des modes repos, VFS et consommation mémoire, succéssivité et préemption, RTOS, MPCore, SMP, mesure d'énergie, multiprocesseurs et basse consommation, ajustement des vitesses processeur, ordonnancement dynamique, mémoire externe et multiprocesseur, bibliographie.
- **Introduction au test numérique** par Michel Renovell
  Contexte, fabrication des circuits intégrés, place du test, comportement du circuit, défaults, pannes, vecteurs de test, test exhaustif, marges, rendement, coût, critères de rentabilité, optimisation de la production, test Go NoGo. variations, tolérances, spécifications, amplitude, sensibilité, spot, modèles de fautes, problèmes au niveau logique, problèmes au niveau temporel, test orienté spécification, test orienté défaut, test numérique, test analogique, structure physique vs structure logique, simulation de faute, générateur automatique de vecteurs de test, conception pour le test, circuit séquenciel, circuit combinatoire, plots de test, test intégré, BIST, LFSR, boundary scan, electronic probing.
- **Les fonctions élémentaires dans un PC : un exemple d'adéquation algorithme-architecture** par Florent de Dinechin
  Fonctions, opérateurs de calcul, qualité numérique du résultat, fonctions de la libm, évaluation logicielle et/ou matérielle, réduction d'argument, approximation polynomiale, normes flottantes, support matériel, FMA multiplication addition fusionnée, exemple IA32, famille Power/PowerPC, famille IA64, optimisation en fréquence et en latence, portabilité vs. performance, astuces d'implantation, détermination des polynômes d'approximation, jeu d'instruction SSE2, parallélisme d'instruction, borner les erreurs, exemple réel, implantation FPGA.
- **Modélisation de SoC avec SystemC** par François Pêcheux
  Contexte, systèmes sur puce, SoC, SoC massivement parallèles, clusters de processeurs, réseau d'interconnection, communication VCI/OCP, réseau sur puce, NoC, plateforme technologique SoCLib, simulation fine, simulation CABA, modèle transactionnel, TLM, modèle de processeur, application embarquée, modèle CABA, modèle de machine d'états, simulation au niveau cycle, machine de Mealy, composant à plusieurs machines d'états, SystemC, SystemCASS, TLM-2.0, parallélisation de la simualtion, granularité, ordonnancement global, horloge locale, synchronisation de processus, transaction bloquante, transaction non-bloquante, phase de transaction, découplage, interconnect compatible, communication par paquets.
- **Performances et programmation des GPU** par David Defour
  Coprocesseur vectoriel, évolution des performances, applications, localité des données, histoire des GPU, parallélisme d'instruction, exemple processeurs Intel, limites de l'augmentation des performances, vectorisation, composants d'un processeur vectoriel, terminologie, modèle d'exécution, optimisations, temps de démarrage, gestion des registres, chaînage, multi-tâches, exécution conditionnelle, gestion de la mémoire, gather/scatter, contraintes sur les accès mémoire, besoin de communication, bus, CUDA, exemples, aspects langages, aspects style de programmation, simulation fonctionnelle, bibliographie.

- **Opérateurs arithmétiques sécurisés** par Arnaud Tisserand
  Terminologie, exemple de chiffrement en crypto symétrique, types d'attaques, attaques théoriques, éviter les attaques théoriques, attaque physique par canaux cachés, quels paramètres mesurer ?, attaque par mesure de la consommation d'énergie, lecture des traces de courant, analyse simple de la consommation (SPA), fonctionnement et limites de la SPA, état interne d'un cryptosystème, analyse différentielle de la consommation (DPA), fonctionnement et exemple de DPA, analyse du rayonnement électromagnétique, attaques par injection de fautes, contre-mesures contre les attaques, opérateurs arithmétiques pour la crypto, arithmétique dans un orps fini premier GF(p), addition modulo (M et $2^n - 1$), multiplication modulaire, exponentiation modulaire, contre-mesure SPA au niveau arithmétique, multiplication scalaire pour ECC, recoder la clé k pour être plus résistant, chaîne d'additions, système double base, représentations des chiffres au niveau circuit, conclusion et perspectives, références.
- **Synthèse de haut niveau** par Bertrand Le Gal
  Introduction et contexte, problématique de la conception, pistes de progrès, introduction à la génération automatique, exemples, implantations variables, automatisation des processus, exploration espace des solutions, construction des circuits numériques, architectures de circuits, instanciation par blocs, flots logiciels, flot de synthèse de haut niveau, contraintes de conception, contraintes d'implémentation, points d'entrées algorithmiques, exemples de codes sources, modèles de représentation foremls, compilation de description algorithmique, extraction parallélisme, propagation des constantes, remplacement d'instructions, déroulage partiel de boucles, style d'écriture, réduction de la compléxité calculatoire, sélection de ressources/opérateurs, bibliothèques, allocation de ressources, allocation orientée par les forces, ordonnancement, mobilité des opérations, assignation sur les ressources, optimisations, fusion d'instruction, dynamique des données, fonctionnalités multiples, placement des données en mémoire, protection propriété intellectuelle, conclusion.
- **Conversion en virgule fixe pour les applications en traitement numérique du signal** par Daniel Ménard
  Introduction, codage des données, codage en virgule fixe et complément à deux, règles de l'arithmétique virgule fixe, exemples, conversion en virgule fixe, étapes du codage, méthodes analytiques, dynamique des données, modèles statistiques, contraintes, méthodes analytiques, détermination position de la virgule, exemple FIR, introduction de bits supplémentaires, recadrage des données, évaluation des performances, sources de bruit, évaluation de la précision, modèles de bruit, puissance du bruit de quantification, exemples, liens codage et synthèse, techniques d'optimisation, exemple sur des DSP, bibliographie.

Intervenants

- **Cécile Belleudy**, Maître de conférence Univ. de Nice
- **Lilian Bossuet**, Maître de conférence ENSEIRB Bordeau
- **Emmanuel Casseau**, Professeur ENSSAT Lannion
- **David Defour**, Maître de conférence Univ. Perpignan
- **Florent de Dinechin**, Maître de conférence ENS Lyon
- **Guy Gogniat**, Professeur Univ. Bretagne Sud
- **Bernard Goossens**, Professeur Univ. Perpignan
- **Vania Joloboff**, Directeur de recherche INRIA Univ. Tsinghua Chine
- **Bertrand Le Gal**, Maître de conférence ENSEIRB Bordeau
- **Daniel Ménard**, Maître de conférence ENSSAT Lannion

- **François Pêcheux**, Maître de conférence Univ. Paris 6
- **Michel Renovell**, Directeur de recherche CNRS LIRMM Montpellier
- **Olivier Sentieys**, Professeur ENSSAT Lannion
- **Arnaud Tisserand**, Chargé de recherche CNRS IRISA Lannion

Posters

9 posters ont été présentés par des doctorants et ATER de la communauté. La présentation des posters durant plusieurs pauses et temps libre autour des repas tout au long de la semaine semble avoir remportée un net succès[1]. De nombreux échanges ont eu lieu autour des posters. Voici la liste de thèmes abordés :

- Utilisation d'un langage à haut niveau d'abstraction : le CAL pour la génération de code hardware et software à destination de cibles reconfigurables, application à un codec h264 SVC (par N. Siret)
- FloPoCo, un générateur de coeurs arithmétiques pour FPGA (par B. Pasca)
- Subword parallelism (SWP) for multimedia operator design (par S. Khan)
- Improving cycle-level modular simulation by vectorization (par M. Bouache)
- How to Make Correct Transaction-level Models (par G. Funchal)
- Architecture flexible pour la stéréovision embarquée (par M. Darouich)
- Simulation fonctionnelle de processeur graphique (par S. Collange)
- Audio ASIP Design for Benchmarking Reconfigurable Processors (par S. Zoghlami)
- Mosaïc : plate-forme de modélisation et de conception d'architectures reconfigurables dynamiquement (par J. Lallet)

Livres de support de cours

L'ensemble des soutiens financiers nous ont permis de proposer un livre de support de cours plus complet pour chaque participant à l'école. Les choix possibles étaient :

- The Designer's Guide to VHDL (3rd ed., 2008). P. Ashenden. 936 pages, Morgan Kaufmann, ISBN-10 : 0120887851
- Architecture de l'ordinateur (5ème éd., 2009). A. Tanenbaum. 733 pages, Pearson Education, ISBN-10 : 2744073776
- CMOS VLSI Design : A Circuits and Systems Perspective (3rd ed., 2004). N. Weste and D. Harris. 800 pages, Addison Wesley, ISBN-10 : 0321149017

4 Bilan des fiches d'évaluation

Une fiche d'évaluation (disponible sur le site web de l'école) a été distribuée à tous les participants. 40 fiches ont été récupérées et analysées.

A—Identification

Type :
- 33 participants
- 7 intervenants

Organismes :
- 5 CNRS

[1]Cette présentation sur beaucoup plus de temps a été préférée à la présentation lors d'une session posters unique.

– 4 INRIA
– 2 Universités

Membre d'une UMR : oui 15, non 8

Statut :
– 21 doctorants
– 4 ingénieurs
– 8 maîtres de conférences
– 1 professeur des universités
– 1 chargé de recherche
– 1 directeur de recherche

Ancienneté dans la recherche : moyenne 6.7 ans

années	0	1	2	3	4	5	8	9	12	15	17	20	28	30
nb personnes.	4	4	6	3	1	2	1	2	1	2	1	1	1	1

Formation initiale :
– 20 informatique
– 11 microélectronique
– 2 traitement du signal
– 2 maths appliquées

B—Inscription

Raison de l'inscription à cette école :
– 26 propre initiative
– 14 incitation directeur de thèse
– 6 incitation organisateurs de l'école
– 1 incitation diverses (bulletin du GDR)

Remarques :
– diffusion sur des listes CNRS inexistante (en particulier à toutes les UMR INST2I) alors que cela avait été fait pour les précédentes éditions.

C—Organisation

Bonne couverture du thème : oui 40, non 0

Qualité : bonne 30, satisfaisante 8, insuffisante 0

Discussions de qualité : oui 38, non 0

Prérecquis clairs : oui 31, non 7

D—Apports

1. 32 mise à jour des connaissances
2. 21 acquisition des concepts de base
3. 17 apport d'informations
4. 6 la connaissance d'un outil
5. 19 synthèse des travaux de recherche actuels

6. 34 une rencontre avec des spécialistes
7. 0 autres

Apport le plus important : 1 (14), 6 (10), 2(7), 5 (3), 3 (2)

E—Moments préférés

- 13 cours
- 20 posters
- 33 repas
- 11 loisirs
- 2 autres (pauses, transports)

F—Contacts avec les intervenants

Oui 40, non 0

Sujets des contacts :
- 28 points du cours
- 34 travaux de recherche respectifs
- 14 projets
- 2 autres (contexte actuel de la recherche en France)

G—Débouchés pour la communauté

- collaborations : oui 9, peut être 27, non 2
- échanges d'informations : oui 24, peut être 13, non 2
- autres :

H—Prolongement souhaité personnellement

1. 22 insertion réseau
2. 29 échanges avec des spécialistes
3. 4 séjour dans un laboratoire
4. 5 réorientation activités de recherche
5. 16 projets de recherche
6. 1 autre formation
7. 1 autres (recrutement postdocs)

Prolongement le plus important : 2 (14), 1 et 5 (4), 4 (3), 7 (1)

I—Souhait d'une suite

Oui 27, non 5
Formes : école, colloque, école avec des ateliers, sujets de stages, séminaires, collaborations.

J—Suggestions générales

Remarques :
- Points positifs : contenu varié, bonne ambiance, cours complémentaires, sessions posters intéressante et animée
- Points négatifs : manque de TP, manque de débats (table ronde), manque de démos d'outils

Cours souhaités (sans ordre) :
- mémoires
- liens architecture et compilation (hard et soft)
- liens matériels et OS
- ordonnancement pour le matériel
- outils de conception de circuits (FPGA et ASIC), en particulier placement/routage
- architecture reconfigurables dynamiquement
- parallélisme (processeur multicœurs)
- réseaux sur puces (NoC)
- modélisation des circuits (vitesse, surface, conso) à haut niveau

Autres souhaits :
- ateliers, TP, démo d'outils ou plateformes
- tutoriaux outils
- propositions de stages (M2R)
- propositions de postdocs
- tables rondes avec les intervenants et tous les participants
- liste des participants avec trombinoscope dès le début de l'école

K—Evaluation thématique

Dans cette partie, il était demandé de noter des rubriques avec une note d'un ensemble de cinq valeurs possibles de 1 (très faible) à 5 (très bon). Les valeurs dans les cases du tableau sont le nombre de personne ayant mis la note de la colonne.

	connaissance					intérêt					
cours	1	2	3	4	5	1	2	3	4	5	souhaits
synthèse h. niv.	2	13	11	8	1	0	1	6	16	11	états outils actuels
crypto. hard	9	12	5	6	3	1	4	4	15	11	
interconnexions	6	10	15	4	2	0	2	8	12	12	
consommation	9	10	17	2	0	1	3	7	8	8	exemples
fonc. élém.	6	16	7	6	2	1	5	8	12	9	
test	11	12	8	7	0	0	2	7	14	14	
SWP	4	11	16	8	1	1	6	8	15	8	
SystemC	9	8	8	5	4	1	4	10	11	9	
compteurs perf.	13	8	8	7	0	0	6	12	8	9	exemples benchmarks
simul. système	10	14	4	6	2	0	2	9	16	8	
FPGA	2	4	11	14	5	0	1	6	17	11	ajouter exploitation
GPU	9	10	10	2	2	1	5	6	13	6	ajouter démo
op. sécurisés	10	12	8	2	1	0	3	6	13	11	ajouter démo
virgule fixe	6	6	7	4	1	1	5	2	10	5	

Remarques :

– prévoir un résumé (et/ou plan) des cours pour mettre sur le web avant l'inscription
– une durée des cours de 2h est un peu trop longue, 1h30 semble plus appropriée.

5 Bilan financier

Tous les montants sont indiqués en Euros TTC (après arrondi).

Recettes	CNRS	8 000
	GDR ARP	4 000
	Lannion Trégor Agglomération	1 500
	Conseil Général 22	900
	INRIA	3 000
	Univ. Rennes 1	1 500
	inscriptions	8 320
	total	**27 220**
Dépenses	hébergement + repas	13 466
	livres supports de cours	3 082
	frais missions intervenants	3 948
	frais organisation	549
	frais gestion INRIA	4 162
	reprographie + fournitures	1 371
	navettes cars + taxi	642
	total	**27 220**

6 Organisation

Comité d'organisation :
– François Charot, INRIA, IRISA
– Elisabeth Lebret, IRISA, Rennes
– Michèle Moizard, ENSSAT
– Sébastien Pillement, IUT Lannion, IRISA
– Olivier Sentieys, ENSSAT, IRISA
– Joëlle Thépault, ENSSAT
– Arnaud Tisserand, CNRS, IRISA

Comité de pilotage scientifique :
– Michel Auguin, LEAT
– François Charot, INRIA, IRISA
– Frédéric Pétrot, UJF
– Pascal Sainrat, IRIT
– Olivier Sentieys, ENSSAT, IRISA
– Arnaud Tisserand, CNRS, IRISA