INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Cairn

Energy Efficient Computing ArchItectures with Embedded Reconfigurable Resources

Rennes - Bretagne-Atlantique

Theme : Architecture and Compiling

Table of contents

1. Team

Research Scientist

François Charot [Research Associate (CR) Inria, Rennes]
Steven Derrien [Associate professor, University of Rennes 1, IFSIC, on leave at Inria since Sept. 2009, Rennes]
Olivier Sentieys [Team Leader, Professor, University of Rennes 1, ENSSAT, on leave (half time) at Inria, Lannion, HdR]
Arnaud Tisserand [Research Associate (CR) CNRS, Lannion]

Faculty Member

Olivier Berder [Associate professor, University of Rennes 1, ENSSAT, Lannion]
Emmanuel Casseau [Professor, University of Rennes 1, ENSSAT, Lannion, HdR]
Daniel Chillet [Associate professor, University of Rennes 1, ENSSAT, Lannion]
Daniel Menard [Associate professor, University of Rennes 1, ENSSAT, Lannion]
Sébastien Pillement [Associate professor, University of Rennes 1, IUT, Lannion]
Stanislaw Piestrak [Professor, on leave from University of Metz at Inria since Sept. 2008, Lannion]
Patrice Quinton [Professor, Director of the Brittany branch of the ENS de Cachan, Rennes, HdR]
Romuald Rocher [Assistant Professor, University of Rennes 1, IUT, Lannion]
Pascal Scalart [Professor, University of Rennes 1, ENSSAT, Lannion, HdR]
Christophe Wolinski [Professor, University of Rennes 1, IFSIC, Rennes, HdR]
Julien Lallet [Lecturer (ATER) until Aug. 2009, IUT, Lannion]

Technical Staff

Charles Wagner [IR CNRS SED, Rennes]
Jérome Astier [Geodes Project, Lannion]
Arnaud Carer [Transmedi@ Project, Lannion]
Thomas Anger [Spring Project, Lannion]
Loïc Cloatre [IA INRIA, ID.Fix Project, Rennes]
Florent Berthelot [RPS2 Project, Rennes]
Amit Kumar [Nano 2012 S2S4HLS Project since Nov. 2009, Rennes]
Jérémie Guidoux [Nano 2012 RECMOTIFS Project since Nov. 2009, Rennes]

PhD Student

Erwan Grace [CEA - University grant, Lannion]
Hai-Nam Nguyen [University grant, Lannion]
Erwan Raffin [CIFRE grant, Thomson, Rennes]
Shafqat Khan [University grant, Lannion]
Kevin Martin [INRIA grant, Rennes]
Manh Pham [Brittany Region - University grant, Lannion]
Michel Thériault [CSRNG Canada grant (co-supervision with Laval University, Québec), Lannion]
Adeel Pasha [MENRT grant, Rennes]
Ludovic Devaux [University grant, Lannion]
Antoine Eiche [University grant, Lannion]
Quoc Tuong Ngo [University grant, Lannion]
Cécile Beaumin-Palud [MENRT grant, Lannion]
Andrei Banciu [CIFRE grant, STMicroelectronics, Grenoble]
Karthick Parashar [Inria Cordi grant, Lannion]
Antoine Floch [Inria grant, Rennes]
Antoine Morvan [Inria grant, Rennes]
Naeem Abbas [Inria grant, Rennes]
Le Quang Vinh Tran [MENRT grant, Lannion]
Chenglong Xiao [Inria grant, Lannion]
Jean-Charles Naud [Inria grant, Lannion]

Matthieu Texier [CEA grant, Saclay]
Thomas Chabrier [University grant, Lannion]
Danuta Pamula [Co-tutelle France-Poland, Lannion]
Robin Bonamy [University grant, Lannion]
Vivek Tovinakere-Dwarakanath [University grant, Lannion]
Mahtab Alam [University grant, Lannion]
Renaud Santoro [MENRT grant (co-supervision with Laval University, Québec) until Dec. 2009, Lannion]
Tuan-Duc Nguyen [University grant until Aug. 2009, Lannion]

Post-Doctoral Fellow

Jérémie Guillot [ROMA Project, Lannion]

Administrative Assistant

Elise Guilloux [Secretary (TR) Inria, Rennes]
Joelle Thépault [Secretary, University of Rennes 1, Enssat, Lannion]

2. Overall Objectives

2.1. Overall Objectives

CAIRN *is a common project with CNRS, University of Rennes 1 (ENSSAT Lannion and IFSIC Rennes) and ENS Cachan-Antenne de Bretagne, and is located on two sites: Rennes and Lannion. The team has been created on January the 1st, 2008 and is a "reconfiguration" of the former R2D2 research team from Irisa.*

The scientific aim of CAIRN is to study hardware and software architectures of *Reconfigurable System-on-Chip (RSoC)*, i.e. integrated chips which include reconfigurable blocks whose hardware configuration may be changed before or even during execution.

Reconfigurable systems have been considered by research in computer science and electrical engineering for about twenty years [90], [98] thanks to the possibilities opened up initially by Field Programmable Gate Arrays (FPGA) technology and more recently by reconfigurable processors [87], [3], [9]. In FPGA, a particular hardware configuration is obtained by loading a bit-stream that is used to shape parameterizable blocks into specific hardware functions. In a reconfigurable processor, coarse-grained logic elements operate on word-size operands and employ reconfigurable operators as computing elements. They are generally tightly coupled with one or more processor cores and act as reconfigurable computing accelerators. Usually, the configuration streams are small enough to ensure run-time – or dynamic – reconfiguration. In a broader sense, hardware reconfiguration may happen not only in a single chip, but also in a distributed hardware system, in order to adapt this system to changing conditions. This happens, for example, on a mobile system.
Recent evolutions in technology and modern hardware systems confirm that reconfigurable chips are increasingly used in modern applications or embedded into more general System-on-Chip (SoC) [118]. Rapidly changing application standards in fields such as communications and information security ask for frequent modifications of the devices. Software updates may often not be sufficient to keep devices in the market, but hardware redesigns are quite expensive. The need to continuously adapt to changing environments (e.g. cognitive radio) is another incentive to use dynamic reconfiguration at runtime. Finally, with technologies at 65 nm and below, manufacturing problems strongly influence electrical parameters of transistors, and transient errors caused by particles or radiations will also more and more often appear during execution: error detection and correction mechanisms or autonomic self-control can benefit from reconfiguration capabilities.

> Standard processors or system-on-chip enable to develop flexible software on fixed hardware.
> Reconfigurable platforms enable to develop ***flexible software on flexible hardware***.

As the density of chips increases [116], power efficiency has become "the Grail" of chip architects: not only for portable devices but also for high-performance general-purpose processors, power (or energy) considerations are as important as the overall performance of the products. This power challenge can only be tackled by using application-specific architectures, or at least by incorporating some application-specific elements into SoCs, as ASICs (Application Specific Integrated Circuit) are much more power-efficient than GPPs (General-Purpose Processor). The designers of SoCs thus face a very difficult challenge: trading between the flexibility of GPP which leads to high-volume and short design time, and the efficiency of ASICs which helps solving the power efficiency problem. Therefore, reconfigurable architectures are often recognized to exhibit the best trade-off potential between power, performance, cost and flexibility [114], [93] because their hardware structure can be adapted to the application needs.

However, reconfigurable systems raise several questions:

- What are the basic elements of a good reconfigurable system? In the early days, they were bit-level operators, and they tend to become word-level operators. There is however no agreement on the model that should be used.
- How can we reconfigure such a system quickly? When to reconfigure? What is the information needed to reconfigure?
- How can we program efficiently reconfigurable systems? We would like to have compilers, not hardware synthesizers and place-and-routers.
- In an application, what must be targeted to reconfigurable chips and what to *conventional* processors? More generally, how can we transform and optimize an algorithm to take advantage of the potential of reconfigurable chips?

The scientific goal of CAIRN is to contribute to answer these questions, based on our background and past experience. To this end, CAIRN intends to approach energy efficient reconfigurable architectures from three angles: the invention of **new reconfigurable platforms**, associated **design and compilation tools**, and the exploration of the **interaction between algorithms and architectures**. Power consumption and processing power are considered as the main constraints in our proposed architecture, design flow and algorithm optimizations, in order to maximize the global energy efficiency of the system.

Wireless Communication is our privileged field of applications. Our research includes the prototyping of parts of these applications on reconfigurable and programmable platforms. Moreover in the framework of research and/or contractual cooperations other **application domains** are considered: image indexing, video processing, cryptography and traffic filtering in high-speed networks.

Members of the CAIRN team have collaborations with large companies like STmicroelectronics (Grenoble), Thomson (Rennes), Thales (Paris), Alcatel (Lannion), France-Telecom Orange Labs (Lannion), Atmel (Nantes), Xilinx (USA), Phillips (NL), Infineon (AU), Omnibase Logic (USA) or SME like Geensys (Nantes), Aphycare Technologies (Lannion), SmartQuantum (Lannion), R-interface (Marseille), Ditocom (Rennes), Sensaris (Grenoble), Envivio (Rennes), Sestream (Paris), Eca-Faros (Lannion). They are involved in several national or international funded projects (ITEA2 Geodes, Nano2012 S2S4HLS and RECMOTIF projects, ANR funded Cifaer, Fosfor, SoCLib, Roma, BioWiic, Open-People and "Pôles de compétitivité" funded Spring, Captiv, Transmedi@, RPS2).

2.2. Highlights

This year, we developed an automatic generation tool for efficient and accurate hardware, on FPGAs or ASICs, evaluation of elementary functions such as reciprocal, square-root, trigonometric, hyperbolic, powers, etc. The obtained circuits are small, fast, and have a low-power consumption. They also provide a good accuracy with bounded maximal error (bounds can be validated using a proof assistant program) or small average error. See Section 6.1.2.

We have defined an original generic approach to the automatic generation of processor reconfigurable extensions and application compilation on these new architectures based on constraints programming. As a result, the two systems UPAK and DURASE were developed and presented at the University Booth of DATE 2009 conference. See Section 6.2.1.
In the fixed-point conversion from floating-point process, one of the main challenge is to evaluate the specification accuracy. We have therefore defined an analytical approach for accuracy estimation of fixed-point embedded systems that allows to obtain precise estimates, much faster than using simulations, the state-of-art approach for this issue. We also defined an automatic floating-point to fixed-point conversion methodology which has been integrated, this year, into an open-source compilation and synthesis framework, and which will be used by companies such as STMicroelectronics. See Section 6.2.3.1.
This year has seen the design and fabrication of an integrated circuit prototype (Ochre: a circuit for On-Chip Randomness Extraction) including our architecture proposal for hybrid random number generator (RNG) [15]. The chip is composed of a TRNG (True RNG) based on several free-running ring-oscillators, a cellular automata PRNG (Pseudo RNG) and some hardware statistical tests including the FIPS 140-2. The tests monitor the TRNG quality in real time to validate the PRNG seed randomness as proposed in [66]. Ochre has been fabricated in a 130 nm CMOS technology from STMicrocelectronics and is able to reach 800 Mbit/s for 0.3mm^2 and 5mW at 200MHz. The circuit has been successfully tested after fabrication. See Section 6.3.7.

Adeel Pasha has won the "Best Student Paper Award" at IEEE INMIC2009 for his paper "Toward Ultra Low-Power Hardware Specialization of a Wireless Sensor Network Node".

3. Scientific Foundations

3.1. Panorama

The development of complex applications is traditionally divided into three steps: theoretical study of the algorithms, study of the target architecture and implementation. When facing new emerging applications such as high-performance, low-power, low-cost mobile communication systems or smart sensor-based systems, it is mandatory to strengthen the design flow by a simultaneous study of both algorithmic and architectural issues[1].

Figure 1 shows the global design flow that we propose to develop. It is organized in levels which refer to our three research themes: application optimization (algorithmic, fixed-point and advanced representations of numbers), platform instance optimization (hardware and middleware), and stepwise refinement and compilation of software tasks (transformations, configuration generation).

In the rest of this part, we briefly describe the challenges concerning **new reconfigurable platforms** in Section 3.2, the issues on **compiler and synthesis tools** related to these platforms in Section 3.3, and the remaining challenges in **algorithm architecture interaction** in Section 3.4.

3.2. Dynamically and Heterogeneous Reconfigurable Platforms

One available technology for building reconfigurable systems is the field-programmable gate arrays (FPGA) introduced to the market in the mid 1980s. Today's components feature millions of gates of programmable logic, and they are dense enough to host complete computing systems on a programmable chip. These FPGAs have been the reconfigurable computing mainstream for a couple of years and achieve flexibility by supporting gate-level reconfigurability, e.g. they can be fully optimized for any application at the bit level. However, their flexibility is achieved at a very important interconnection cost. To be configured, a large amount of data must be distributed via a slow serial programming process to all the processing and interconnection resources. Configurations must be stored in an external memory. These interconnection and configuration overheads lead to energy inefficient architectures.

[1] Often referenced as algorithm-architecture mapping or interaction.

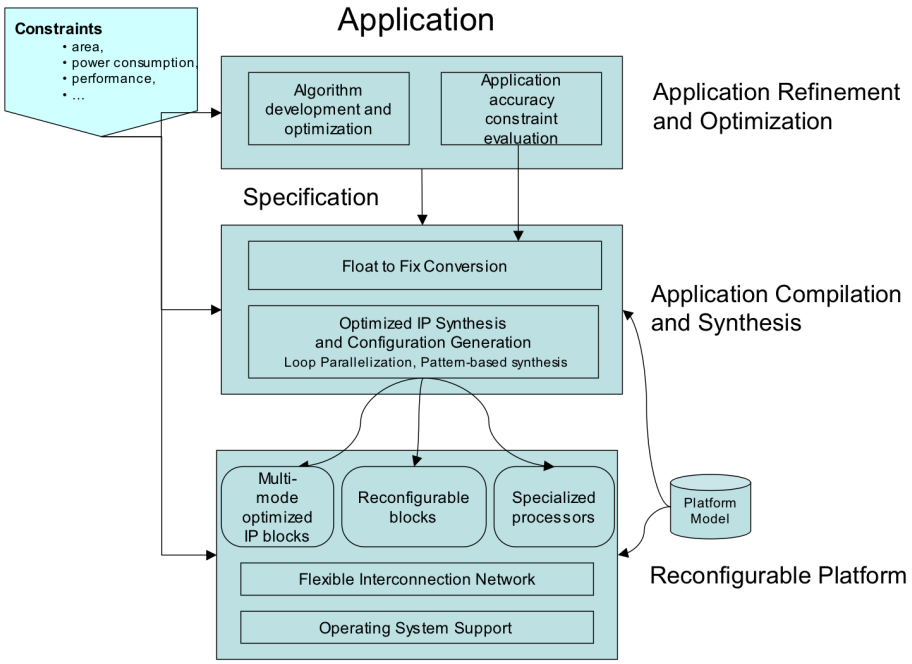

Figure 1. CAIRN*'s general design flow and related research themes*

To increase optimization potential of programmable processors without the FPGAs penalties, the functional-level reconfiguration was introduced. *Reconfigurable Processors* are the most advanced class of reconfigurable architectures. The main concern of this class of architectures is to support flexibility while reducing reconfiguration overhead. Precursors of this class were the KressArray [99], RaPid [96], and RaW machines [120] which were specifically designed for streaming algorithms. Morphosys [104], Remarc [109] or Adres [94] contain programmable ALUs with a reconfigurable interconnect. These works have led to commercial products such as the Extreme Processor Platform (XPP) [86] from PACT, Bresca [112] from Silicon Hive, designed mainly for telecommunication applications.
Another strong trend towards heterogeneous reconfigurable processors can be observed. Hybrid architectures combine standard GPP or DSP cores with arrays of *field-configurable elements*. These new reconfigurable architectures are entering the commercial market. Some of their benefits are the following: functionality on demands (set-top boxes for digital TV equipped with decoding hardware on demand), acceleration on demand (coprocessors that accelerate computationally demanding applications in multimedia, communications applications), and shorter time to market (products that target ASIC platforms can be released earlier using reconfigurable hardware).
Dynamic reconfiguration allows an architecture to adapt itself to various incoming tasks. This requires complex management and control which can be provided as services of a real-time operating system (RTOS) [105]: communication, memory management, task scheduling [92] [89] and task placement [84]. Such an Operating System (OS) approach has many advantages: it is a complete design framework, independent of the technology and of the hardware architecture, thus helping to drastically reduce the design time of the complete platform.

Communications in a reconfigurable platform is also a very important research subject. The role of communication resources is to support transactions between the different components of the platform, either between macro-components of the platform – main processor, dedicated modules, dynamically reconfigurable parts of

the platform – or inside the elements of the reconfigurable parts themselves. This has motivated studies on Networks on Chip for Reconfigurable SoCs [88] [111] that trade flexibility and quality of service.

In CAIRN we mainly target reconfigurable system-on-chip (RSoC) defined as a set of computing and storing resources organized around a flexible interconnection network and integrated onto a single silicon chip (or programmable chip such as FPGAs). The architecture is specialized for an application domain, and the flexibility is featured by hardware reconfiguration and software programmability. Therefore, computing resources are heterogeneous and we focus on the following:

- **Reconfigurable hardware blocks with a dynamic behavior** where reconfigurability can be achieved at the bit or at the operator level. Our research aims at defining new reconfigurable computing and storing resources. Since reconfiguration must occur as fast as possible (typically a few cycles), the reduction of the configuration bit-stream length is also a key issue.
- When performance and power consumption are major constraints, it is well known that optimized specialized hardware blocks (often called IPs for Intellectual Properties) are the best (and often the only) solution. As a flexible extension of specialized IPs, we study **multi-mode components** for very specific set of high-complexity algorithms, without loss of performance.
- Specialized **processors with tailored instruction-set** still offer a viable solution to trade between energy efficiency and flexibility. They are especially interesting in the context of recent FPGA platforms where multiple processors can be easily embedded. We also focus on the automatic generation of an optimized customized instruction-set and of the associated data-path and interface with an embedded processor core.

3.3. Compilation and Synthesis for Reconfigurable Platform

The absence of compilers is one of the major limitations for the use of reconfigurable architectures in real-life applications. Therefore, the ability to compile and optimize code on reconfigurable hardware platforms from high-level specifications is the key for a real success story and is a hot topic in the research community. We continue our research efforts to offer **efficient tools with close links to architectures**.

Most current programming environments for reconfigurable systems consist of separate tool flows for the software and the hardware. Processor code and configuration data for the reconfigurable processing units are handcrafted and wrapped into libraries of functions. Progress beyond current practices calls for compilers capable of generating code and configurations from a high-level general-purpose programming language. Such a compiler decides which operations go into the reconfigurable processors. Loops or frequently executed code fragments are good candidates for reconfigurable platforms. For general-purpose code, this leads to several problems: it is difficult to extract sets of operations with matching granularity at a sufficient level of parallelism; inner loops of general-purpose programs often contain excess code; i.e. code that must be run on a CPU such as exceptions, function or system calls. Efforts aimed at automatic code generation for reconfigurable architectures include works of [110], [119] and [122].

Another approach to programming and design of reconfigurable platform, especially for special-purpose elements, is to use techniques inspired from high-level synthesis. Here also, loops are the target of the methods: the goal is to either generate special-purpose architectures made out of arithmetic operators or to produce parallel architectures. In both cases, the output may be either efficient special-purpose hardware for computation-intensive tasks and/or the parameters for a reconfigurable architecture. Such approaches will eventually create a bridge between compilation techniques and hardware design.

Finally, we continue to investigate floating-point to fixed-point automatic conversion with the objective to develop an open-source tool. Multimedia and signal processing are main application fields for reconfigurable platforms. In general, these algorithms are specified using floating-point operations, but, for efficiency reasons, they are often implemented with fixed-point operations either in software for DSP cores or as special-purpose hardware. Unfortunately, fixed-point conversion is very challenging and time-consuming, typically demanding 25 to 50% of the total design or implementation time[2]. Thus, tools are required to automate this conversion.

In software implementations (DSP, MCU), the aim is to define an optimized fixed-point specification which minimizes the code size and the execution time for a given computation accuracy constraint. This optimization is achieved through the modification of the scaling operation location and the selection of the data word-length according to the different data-types supported by DSPs. In hardware implementations (ASIC, FPGA), the complete architecture has to be defined. The efficient implementation requires to minimize the architecture size and the power consumption. Thus, the conversion process goal is to minimize the operator word-length. In the fixed-point conversion process, one of the main challenge is to evaluate the fixed-point specification accuracy. For DSP-software implementation, methodologies have been proposed [102], [108], [107] to achieve a floating-point to fixed-point conversion leading to an ANSI-C code with integer data types. One of the key is to closely link the compilation flow to the latest DSP features. For hardware implementation, the best results are obtained when the word-length optimization process is coupled with the high-level synthesis [101] [91].

3.4. Algorithm Architecture Interaction

As CAIRN focus on domain-specific systems-on-chip including reconfigurable capabilities, algorithmic-level optimizations have a great potential on the efficiency of the overall system. Based on the skills and experiences in "signal processing and communications" of some CAIRN's members, we conduct research on algorithmic optimization techniques under two main constraints: energy consumption and computation accuracy; and for two main application domains: fourth-generation (4G) mobile telecommunications and wireless sensor networks (WSN). These application domains are very conducive to our research activities. The high complexity of the first one and the stringent power constraint of the second one, require the design of specific high-performance and energy efficient SoCs. Sections 4.1 to 4.5 detail the application domains that we focus on.

We also work on computer arithmetic operators and representations of numbers for hardware and software implementations. We provide algorithms for evaluating operations such as: addition, multiplication, multiplication by constant, power, division, roots, (inverse) trigonometric functions, (inverse) hyperbolic functions, logarithms, exponentials, and combinations. For hardware implementations, we work on the reduction of the delay, silicon area and power consumption. For software implementations, we focus on high-performance computing libraries on general purpose processors (GPPs) and graphic processor units (GPUs). We work on the use of exotic representations of numbers in specific domains such as secured implementations of cryptosystems with high-performance protection against side-channel analysis or fault attacks.

4. Application Domains

4.1. Panorama

Our research is based on realistic applications, in order to both discover the main needs created by these applications and to invent realistic and interesting solutions.

The high complexity of the **Next-Generation (4G) Wireless Communication Systems** leads to the design of real-time high-performance specific architectures. The study of these techniques is one of the main field of applications for our research, based on our experience on WCDMA for 3G implementation.

In **Wireless Sensor Networks** (WSN), where each wireless node has to operate without battery replacement for a long time, energy consumption is the most important constraint. In this domain, we mainly study energy-efficient architectures and wireless cooperative techniques for WSN.

Intelligent Transportation Systems (ITS), and especially Automotive Systems, more and more apply technology advances. While wireless transmissions allow a car to communicate with another or even with road infrastructure, **automotive industry** can also propose driver assistance and more secure vehicles thanks to improvements in computation accuracy for embedded systems.

[2] http://www.mathworks.com/company/newsletters/digest/may04/uwb.html

Other important fields will also be considered: specialized hardware systems for the filtering of the network traffic at high-speed, high-speed true-random number generation for security, content-based image retrieval and video processing.

4.2. 4G Wireless Communication Systems

With the advent of the next generation (4G) broadband wireless communications, the combination of MIMO (Multiple-Input Multiple-Output) wireless technology with Multi-Carrier CDMA (MC-CDMA) has been recognized as one of the most promising techniques to support high data rate and high performance. Moreover, future mobile devices will have to propose interoperability between wireless communication standards (4G, WiMax ...) and then implement MIMO pre-coding, already used by WiMax standard. Finally, in order to maximize mobile devices lifetime and guarantee quality of services to consumers, 4G systems will certainly use cooperative MIMO schemes or MIMO relays. Our research activity focuses on MIMO pre-coding and MIMO cooperative communications with the aim of algorithmic optimization and implementation prototyping.

4.3. Wireless Sensor Networks

Sensor networks are a very dynamic domain of research due, on the one hand, to the opportunity to develop innovative applications that are linked to a specific environment, and on the other hand to the challenge of designing totally autonomous communicating objects. Cross-layer optimizations lead to energy-efficient architectures and cooperative techniques dedicated to sensor networks applications.

4.4. Automotive Systems

Technology advances, for embedded devices inside vehicles or communication systems between vehicles (V2V) or with road infrastructure (V2R), allow to significantly improve the security of drivers and road users.

One of our goals is to propose new low-cost and energy-efficient mobile communication solutions to ease and make safer road traffic conditions. Considering "intelligent" road signs and vehicles, i.e. equipped with an autonomous radio communication system, drivers will be able to receive at any time various information about traffic fluidity or road signs identification. In particular, cooperative MIMO techniques are used to decrease the energy consumption of the communications.

Other research related to automative systems is for example the design of proved accurate fixed-point controllers.

4.5. Multimedia processing

In multimedia applications, audio and video processing is the major challenge embedded systems have to face. It is computationally intensive with power requirements to meet. Video or image processing at pixel level, like image filtering, edge detection and pixel correlation or at bloc level such as transforms, quantization, entropy coding and motion estimation have to be accelerated. We investigate the potential of reconfigurable architectures for the design of efficient and flexible accelerators in the context of multimedia applications.

5. Software

5.1. Panorama

Besides the development of new reconfigurable architectures, the need for efficient compilation flow is stronger than ever. Challenges come from the high parallelism of these architectures and also from new constraints such as resource heterogeneity, memory hierarchy and power constraints and management. We aim at defining a highly effective software framework for the compilation of high-level specifications into optimized code executed on a reconfigurable hardware platform. Figure 2 shows the global framework that we are currently developing.

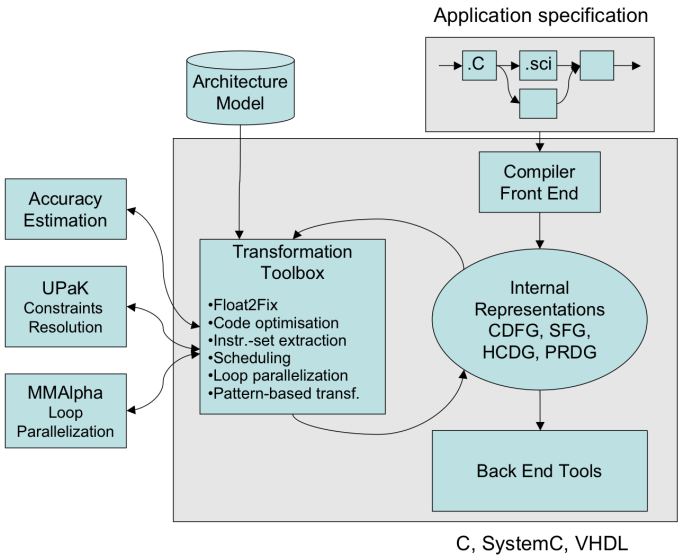

Figure 2. CAIRN*'s general software development framework*

Our approach assumes that the application is specified as a hierarchical block diagram of communicating tasks expressing data-flow or control, where each task is expressed using languages like C, Signal, Scilab or Matlab, and is then transformed into an internal representation by the compiler front-end. Then, our framework is based on applying some high-level transformations onto the internal representation.

Different internal representations are used depending on the targeted transformations or the targeted architectures.

- The classical Control and Data Flow Graph (CDFG) is the main internal formalism of our framework. It is the basis for transformations like code optimizations, fixed-point transformations, instruction-set extraction or scheduling. Gateways will be provided from CDFG to other supported formalisms.
- The Hierarchical Conditional Dependency Graph (HCDG) format[3] will be used as the internal representation for pattern-based transformations.
- Other internal representations like Signal Flow Graphs (SFG) and Polyhedral Reduced Dependence Graph (PRDG) will be used respectively for application accuracy estimation and loop parallelization techniques.

Finally, back-end tools enable the generation of code like VHDL for the hardwired or reconfigurable blocks, C for embedded processor software, and SystemC for simulation purposes (e.g. fixed-point simulations). The compiler front-end, the back-end generators, the transformation toolbox as well as the different internal representations and their respective gateways are based on a single framework: the Gecos framework.

Besides CAIRN's general design workflow, and in order to promote research undertaken by CAIRN, several hardware and software prototypes are developed. Among those, some distributed software are presented in this report: Gecos a flexible compilation platform, ID.Fix an infrastructure for the automatic transformation of software code aiming at the conversion of floating-point data types into a fixed-point representation, UPaK and

[3] as defined in the Polychrony http://www.irisa.fr/espresso/Polychrony/ toolset

Durase for the compilation and the synthesis targeting reconfigurable platforms, and Interconnect Explorer a high-level power and delay estimation tool for on-chip interconnects.

5.2. Gecos

Participants: Steven Derrien [correspondant], Daniel Ménard, Kevin Martin, Antoine Floch, Antoine Morvan, Adeel Pasha, Patrice Quinton, Amit Kumar, Loïc Cloatre.

The Gecos (Generic Compiler Suite) project is an open source Eclipse-based C compiler infrastructure developed in the CAIRN group since 2004 that allows for fast prototyping of complex compiler passes. Gecos was designed so as to address part of the shortcomings of existing C/C++ infrastructures such as SUIF and LLVM.

Gecos is a 100% Java based implementation and is based on modern software engineering practices. It uses Eclipse plugin as an underlying infrastructure and thus takes benefits of its plugin mechanism to be easily extensible. So as to benefit from all the benefits of Model Driven Software Engineering techniques, we now also offer a EMF (Eclipse Modeling Framework) based version of the compiler intermediate representation, and plan to base all subsequent developments on MDE technologies.

The Gecos infrastructure is still under very active development, and now serves as a backbone infrastructure to many group members (Upak, Durase, ID.Fix). In 2009, the work has focused on retargeting the infrastructure for source to source transformation, in the context of the Nano2012-S2S4HLS project in collaboration with STMicroelectronics. The Gecos compiler framework is open-source and is hosted on the INRIA gforge http://gecos.gforge.inria.fr.

5.3. ID.Fix: Infrastructure for the Design of Fixed-point Systems

Participants: Daniel Ménard [correspondant], Olivier Sentieys, Romuald Rocher, Loic Cloatre, Jérémie Guillot.

In parallel to the definition of the fixed-point conversion methodology an infrastructure for the design of fixed-point systems is under development to provide an optimized fixed-point specification from the application description. The application is described with a C code using floating-point types. The tool generates a C code using fixed-point data types (`ac_fixed`) from Mentor Graphics. The infrastructure is made-up of three main modules corresponding to the fixed-point conversion (Fix.Conv), the accuracy evaluation (Acc.Eval) and the dynamic range evaluation (Dyn.Eval). This year, the module Acc.Eval for evaluating the fixed-point accuracy has been developed. The first version supports linear-time invariant systems. The next version will be developed in 2010 and will support any system based on arithmetic operations. The Fix.Conv module for the fixed-point conversion is under development inside the Gecos framework. The development of this tool is achieved thanks to an INRIA graduate engineer in the context of S2S4HLS project and a CNRS graduate engineer since September 2009 in the context of ROMA ANR project.

5.4. UPaK: Abstract Unified Pattern-Based Synthesis Kernel for Hardware and Software Systems

Participants: Christophe Wolinki [correspondant], François Charot, Kevin Martin, Antoine Floch.

We are developing (with strong collaboration of Lund University, Sweden and Queensland University, Australia) UPaK *Abstract Unified Pattern Based Synthesis Kernel for Hardware and Software Systems* [121]. The preliminary experimental results obtained by the UPak system show that the methods employed in the systems enable a high coverage of application graphs with small quantities of patterns. Moreover, high application execution speed-ups are ensured, both for sequential and parallel application execution with processor extensions implementing the selected patterns. UPaK is one of the basis for our research on compilation and synthesis for reconfigurable platforms. It is based on the HCDG representation of the Polychrony software designed at INRIA-Rennes in the project-team Espresso.

5.5. DURASE: Automatic Synthesis of Application-Specific Processor Extensions

Participants: Christophe Wolinki [correspondant], François Charot, Kevin Martin, Antoine Floch.

We are developing a framework enabling the automatic synthesis of application specific processor extensions. It uses advanced technologies, such as algorithms for graph matching and graph merging together with constraints programming methods. The framework is organized around several modules.

- CoSaP: Constraint Satisfaction Problem. The goal of CoSaP is to decouple the statement of a constraint satisfaction problem from the solver used to solve it. The CoSaP model is an Eclipse plugin described using EMF to take advantage of the automatic code generation and of various EMF tools.
- HCDG: Hierarchical Conditional Dependency Graph. HCDG is an intermediate representation mixing control and data flow in a single acyclic representation. The control flow is represented as hierarchical guards specifying the execution or the definition conditions of nodes. It can be used in the gecos compilation framework via a specific pass which translates a CDFG representation into an HCDG.
- Patterns: Flexible tools for identification of computational pattern in a graph and graph covering. These tools model the concept of pattern in a graph and provide generic algorithms for the identification of pattern and the covering of a graph. The following sub-problems are addressed: (sub)-graphs isomorphism, patterns generation under constraints, covering of a graph using a library of patterns. Most of the implemented algorithms use constraints programming and rely on the CoSaP module to solve the optimization problem.

5.6. PowWow: Power Optimized Hardware and Software FrameWork for Wireless Motes

Participants: Olivier Sentieys [correspondant], Olivier Berder, Thomas Anger, Arnaud Carer, Jérôme Astier, Samuel Mouget, Adeel Pasha, Steven Derrien.

PowWow is a hardware and software platform designed to handle wireless sensor network (WSN) protocols and related applications. Based on an asynchronous rendezvous medium access (MAC) protocol, geographical routing and `protothread` library, PowWow requires a lighter hardware system than Zigbee [85] to be processed (memory usage including application is less than 10kb). Therefore, network lifetime is increased and price per node is significantly decreased.

CAIRN's hardware platform (see Figure 3) is composed of:

- The motherboard, designed to reduce power consumption of sensor nodes, embeds an MSP430 microcontroller and all needed components to process PowWow protocol except radio chip. JTAG, RS232, and I2C interfaces are available on this board.
- The radio chip daughter board is currently based on a TI CC2420.
- The coprocessing daughter board includes a low-power FPGA which allows for hardware acceleration for some PowWow features and also includes dynamic voltage scaling features to increase power efficiency. The current version of PowWow integrates an Actel IGLOO AGL250 FPGA and a programmable DC-DC converter. We have shown that gains in energy of up to 700 can be obtained by using FPGA acceleration on functions like CRC-32 or error detection with regards to a software implementation on the MSP430.

PowWow distribution also includes a generic software architecture using event-driven programming and organized into protocol layers (PHY, MAC, LINK, NET and APP). The software is based on Contiki [95], and more precisely on the `Protothread` library which provides a sequential control flow without complex state machines or full multi-threading.

Figure 3. CAIRN*'s PowWow motherboard with radio board connected*

To optimize the network regarding a particular application and to define a global strategy to reduce energy, PowWow offers the following extra tools: over-the-air reprogramming (and soon reconfiguration), analytical power estimation based on software profiling and power measurements, a dedicated network analyzer to probe and fix transmissions errors in the network. More information can be found at http://powwow.gforge.inria.fr.

5.7. Interconnect Explorer: a High-Level Power and Delay Estimation Tool for On-Chip Interconnects

Participants: Antoine Courtay [correspondant], Olivier Sentieys, Johann Laurent [Lab-Sticc, Lorient].

In today's SoCs, interconnects introduce delays and consume power and chip resources. A tool, called Interconnect Explorer, has been developed for high-level estimation of interconnect performance which provides fast and accurate figures for both time and power consumption [2]. These results allowed us to determine new key issues that have to be taken into account for future performance optimizations. This tool is based on energy and timing multi-input tables obtained from transistor-level simulations. The tool can be configured by setting the following parameters: technology, metal layer, bus length, bus width, frequency, and bufferization type. Interconnect Explorer provides users with results in terms of energy consumption, static power consumption, average dynamic power consumption, maximum dynamic power consumption, instantaneous dynamic power consumption, maximum frequency allowed on the bus, area of the bus (wires and buffers), commutation rate per bit and percentage of appearance of each type of transitions. The maximum error between consumption results provided by Interconnect Explorer and SPICE simulation is less than 6%. Interconnect Explorer provides results instantaneously (less than 1 second computation) whereas a SPICE simulation of the same configuration takes several hours.

5.8. SoCLib: Open Platform for Virtual Prototyping of Multi-Processors System on Chip

Participants: François Charot [correspondant], Laurent Perraudeau, Charles Wagner.

SoCLib is an open platform for virtual prototyping of multi-processors system on chip (MP-SoC) developed in the framework of the SoCLib ANR project. The core of the platform is a library of SystemC simulation models for virtual components (IP cores), with a guaranteed path to silicon. All simulation models are written in SystemC, and can be simulated with the standard SystemC simulation environment distributed by the OSCI organization. Two types of models are available for each IP-core: CABA (Cycle Accurate / Bit Accurate), and TLM-DT (Transaction Level Modeling with Distributed Time). All simulation models are distributed as free software. We have developed the simulation model of the NIOSII processor, of the Altera Avalon interconnect, and of the TMS320C62 DSP processor from Texas Instruments. Find more information on its dedicated web page: http://www.soclib.fr.

5.9. LDPC-Dec-DVBS2: Low Density Parity Code (LDPC) Decoder Architecture

Participants: François Charot [correspondant], Florent Berthelot.

LDPC-Dec-DVBS2 is an RTL model in the VHDL hardware description language of a LDPC decoder for the digital video broadcast DVB-S2 standard. LDPC-Dec-DVBS2 is implemented as a synthesizable VHDL model. It is capable of processing all specified code rates of the DVB standard. This model is developed in the framework of the RPS2 project.

5.10. OCHRE: On-Chip Randomness Extraction

Participants: Olivier Sentieys [correspondant], Renaud Santoro, Thomas Anger, Arnaud Carer.

Ochre is a set of synthesizable VHDL models for true and pseudo random number generation and hardware accelerated statistical tests. It includes IP cores of different oscillator-based TRNGs, different PRNGs (linear feedback shift registers, cellular automata, AES) and several statistical tests (FIPS 140-2, AIS31, Diehard). This set of IPs has been used to design Ochre V1 and V2 chips and are delivered under GNU GPL license.

6. New Results

6.1. Dynamically and Heterogeneous Reconfigurable Platforms

6.1.1. New Reconfigurable Architectures

6.1.1.1. Flexible Arithmetic Operator Design

Participants: Emmanuel Casseau, Daniel Ménard, François Charot, Christophe Wolinski, Shafqat Khan.

Our aim is to propose new arithmetic operators flexible in term of data size. Targeted applications are typically multimedia processing. To optimize fixed-point implementations, architectures must offer operators which support different data word-lengths. Operator efficiency can be increased using subword parallelism (SWP) scheme. A single SWP instruction performs the same operation on multiple sets of subwords in parallel using SWP operators. In the existing SWP capable processors, the choices for subword data sizes are usually 8, 16, 32 bits etc. The reason behind the selection of these subword sizes being the less complexity of SWP operator design especially when subword sizes are multiple of the smallest subword size. However in multimedia applications, the input data (pixels) for computations are 8, 10, 12 and sometimes 16 bits. These multimedia data sizes are not in coordination with existing processor's subword sizes resulting in the under utilization of processor resources. Operators which can support multimedia oriented subword sizes (8, 10, 12 and 16) are required. Multimedia operations are based on basic operators (add, absolute value, multiply) but more complex operations are also required to increase both speed an efficiency. For instance $\sum |a-b|$ operation is required in the calculation of SAD, $\sum(a \times b)$ operation is required for the multiplication-accumulation operation used in the DCT algorithm etc. To overcome the overheads of reconfigurations such as the complexity of the interconnection network and the reconfiguration time, we designed a pipelined multimedia operator which provides reconfigurability inside the operator using a configurable datapath [46]. The operator can be configured to perform most of multimedia operations on different data sizes without any need of reconfiguration time. This operator will be used as one computing unit inside a reconfigurable processor tailored for multimedia applications [52].

6.1.1.2. Adaptive and Multi-mode Devices

Participants: Emmanuel Casseau, Antoine Floch, Erwan Raffin, Daniel Ménard, Shafqat Khan, François Charot, Christophe Wolinski, Olivier Sentieys.

In a mobile society, more and more devices need to continuously adapt to changing environments that is to say devices will have to be flexible to implement different algorithms at different times. Such mode switches require more than just software based changes but also adaptation of the application specific hardware components. To issue this requirement, we investigate two ways. The first one is the design of a reconfigurable processor able to adapt its computing structure to a dedicated domain: video and image processing applications. The processor is built around a pipeline of coarse grain reconfigurable operators exhibiting a good trade-off between performance and power consumption. On the contrary of what has been done in previous reconfigurable processors, flexibility is not obtained through the use of a flexible interconnect network but on the use of configurable domain-dedicated units [52]. This work is done in the context of the ROMA ANR project. We particularly investigate reconfigurable operator design and compilation framework. The second way is the synthesis of multi-mode architectures which do not lead to any reconfiguration time penalty. Such architectures implement all required operators according to the pre-defined set of computations to be performed. In order to optimize area, these operators are shared between the set of algorithms, and some control logic steers the data to operators depending on the particular algorithm to be executed at a specific time. Syntheses can be constrained for performance or area. Targeted domains are typically channel encoding, cryptography and multimedia [43]. This work is done through a collaboration with IMS Lab. (B. Le Gal).

6.1.1.3. Reconfigurable Architecture Description Language

Participants: Julien Lallet, Sébastien Pillement, Olivier Sentieys, François Charot.

Our research aims at defining a platform model for the definition of dynamically reconfigurable architectures and associated methods. The main objective is to have a unified and formal specification of the platform that can be efficiently exploited in retargetable compilation flows, and in automated back-end generators for simulation and synthesis. The model is defined to cover different models of architectures, from FPGAs to networks of processors, through coarse-grained reconfigurable data-path.

This method allows to easily develop a new dynamically reconfigurable architecture based on computing resources and generic interconnection schemes, to explore performance and to validate the architecture by simulations at different levels of abstraction. The definition of the architecture is done with the help of a high-level architecture description based on the MAML language developed at the University of Erlangen-Nuremberg. The first part of the work defined structures that permit to interconnect different kinds of computing resources (configurable logic blocks, reconfigurable functional units or processors) and to produce the required reconfiguration resources for an homogeneous reconfiguration process. Different architecture paradigms (FPGA, reconfigurable datapaths such as DART or regular parallel processor architectures such as WPPA) can thus be quickly modeled. The second part of this work consisted in the generation of the configuration controller, after analyzing the MAML specifications of the architecture and of the reconfiguration resources produced. This work leads to the development of the Mozaic framework. This tool is able to generate a reconfigurable platform and to explore some important parameters (reconfiguration costs and time, flexibility and size of interconnect, number of resources). The proposed reconfiguration paradigm for computing and interconnect resources has been optimized for very fast reconfiguration process, which is essential to reach the timing constraint required by today's applications. Implementation of a wireless receiver has been tested on various architectures generated by our tool and has shown the efficiency of our methodology applied to reconfigurable systems [19], [48], [73].

6.1.2. Arithmetic Operators and Number Representations

Participants: Arnaud Tisserand, Stanislaw Piestrak.

6.1.2.1. Arithmetic Operators for Cryptography

Redundant number systems have been introduced to speed-up some computations. In a redundant number system, some numbers have several distinct representations. This property is used in some number systems to allow constant time addition (the addition time does not depend on the number of digits). Redundant number systems have been used in cryptography for a long time. Recodings of some values into a redundant number system are frequent. For instance, Non-Adjacent Forms (NAF and w-NAF) are used in modular exponentiation in RSA and in scalar multiplication in ECC. Redundancy is used to lower the number of some operations. In [82] and [31] we present some investigations on links between redundant number systems and reconfigurable arithmetic units with countermeasures against some side channel attacks. The use of redundant number system allows to change the way some computations are performed (and then their effects on side channel analysis/attacks). The frequency (internal iteration level, field operation level, curve operation level...) and the location (digit level, number level, curve point level...) of the reconfigurations widely impact units characteristics. We present first results on reconfigurable arithmetic units for cryptography.

6.1.2.2. Dedicated Arithmetic Operators

In [68], we study the design of dedicated function approximation operators based on the mix of two recent techniques: low-degree polynomial approximation proposed in [11] and estimated arithmetic operators proposed in [113]. The method proposed in [11] allows to design operators for function approximation dedicated to hardware implementation. The generated operators use low-degree polynomial approximations where the coefficients are selected for accuracy and implementation purpose. Estimated arithmetic proposed in [113] deals with arithmetic circuits with approximated result. Some internal signals such as carries are not computed. Estimated arithmetic trades accuracy for speed, silicon area and power. Adders and multipliers have been investigated using estimated arithmetic. In [68], we study various trade-offs between the degree of the polynomial, its coefficients selection, the data-path size and the accuracy of the estimated arithmetic operators. The obtained operators are small and fast, and they provide a small average error but a few large errors may occur for some very infrequent arguments. Typical delay improvements are about 20–60% and 15–30% area reduction compared to previous results.

6.1.2.3. Number Representation for Digital Signal Processing (DSP)

Two's complement number systems impose a fundamental limitation on the power and performance of arithmetic circuits, due to the fundamental need of cross-datapath carry propagation. Residue Number System (RNS) breaks free of these bonds by decomposing a number into parts and performing arithmetic operations in parallel. In [34], we proposed to extend the instruction set architecture with separate instructions for RNS computations. The basic RNS components were designed in RTL Verilog and synthesized using the 0,18μ OSU standard cell library with the Cadence Encounter ® RTL Compiler. An application mapping problem on the proposed RNS extension that includes both instruction selection and instruction scheduling was formulated and solved. Our experiments not only demonstrate simultaneous improvement of up to 30% in performance and 57% reduction in functional unit power consumption, but also that most of these benefits can be exploited with automatically generated code. The compiler technique introduced in this work could also benefit from improving the profit model to model instruction execution more accurately. The limitations of RNS include difficult implementation of non-modular operations like magnitude comparison, sign detection, and division. To alleviate these drawbacks, the diagonal function was proposed by Dimauro *et al.* However, in [22], we have shown that any implementation involving the diagonal function proposed to date actually results in excessive hardware overhead and delay, which make it impractical from the application view, so that it cannot compete with more traditional approaches.

6.1.3. Management of Dynamically Reconfigurable Systems

Participants: Antoine Eiche, Daniel Chillet, Sébastien Pillement, Ludovic Devaux, Olivier Sentieys.

To support the dynamic behavior of new embedded applications, heterogeneous execution resources are often included in modern SoC or MPSoC (Multi-Processor System-on-Chip) systems. The management of these resources is classically supported by an operating system (OS) that includes several specific services. One new needed service concerns the task scheduling and placement within the reconfigurable resources. The classical

temporal scheduling problem is then extended with a spatial dimension in order to manage the physical available area into the reconfigurable resource. The second impacted service is the task communication management. The on-line task placement makes the interconnection support difficult to predict. Then, a flexible and dynamically interconnect medium must be defined.

6.1.3.1. Models for Dynamically Reconfigurable Systems

Participants: Daniel Chillet, Sébastien Pillement.

During the high-level design of the complete system, the designer must be able to choose between different architecture, application and operating system solutions. To support the exploration phase, the OverSoC project has proposed to develop a global methodology. In this context, we developed a first model of a dynamically reconfigurable architecture (DRA). Built using SystemC language, the model is modular and permits the fast evaluation of specific OS services for DRA management [64]. Based on this model, we implemented several services, such as a simple task placement, and evaluated several design parameters to qualify solutions [79]. The model is effective and was integrated in the OverSoC methodology.

6.1.3.2. Scheduling based on Artificial Neural Networks

Participants: Antoine Eiche, Daniel Chillet, Sébastien Pillement, Olivier Sentieys.

During this year, we continued our work on scheduling through Artificial Neural Networks (ANN) and we compared classical scheduling algorithms (e.g. PFair) and our ANN structure composed of inhibitor neurons. We have demonstrated that our model can manage heterogeneous multiprocessor architectures while classical scheduling solutions are only applicable for homogeneous multiprocessors [28], [16]. Our scheduling was extended with task placement on heterogeneous reconfigurable execution resource by defining a spatio-temporal scheduling composed of two steps. The first step is the time scheduling under a resource placement constraint. The second step is the task placement with a real model of the possible instances of each application task. These two steps are solved by two different neural networks which can be evaluated in parallel [72]. A hardware structure of our neural network has been developed for the temporal scheduler and shows that hardware implementation is very efficient and can be a very good candidate for hardware implementation of this service.

6.1.3.3. Flexible Communication Infrastructure

Participants: Daniel Chillet, Sébastien Pillement, Ludovic Devaux.

For task communication within reconfigurable resources, we defined a specific interconnection architecture adapted to dynamically and partially reconfiguration resources included into modern SoC. We defined a first hierarchical interconnect infrastructure and specified an RTL VHDL model of this solution. Furthermore, to evaluate our architectural proposal, we built a demonstrator platform which allows us to illustrate the reconfiguration concept of the communication network. This leads to the DRAFT network based on the fat-tree topology, specifically designed to support the communication constraints required by the dynamic reconfiguration [41]. DRAGOON, an automatic generator of DRAFT simulation and synthesis models, was also designed to evaluate various versions of the network. Thanks to DRAGOON, DRAFT has successfully been compared with most popular Network-on-Chip (NoC) topologies, like mesh and regular fat-tree [18].

6.1.4. Fault-Tolerant Reconfigurable Systems

Participants: Stanislaw Piestrak, Sébastien Pillement, Manh Pham, Olivier Sentieys.

The use of reconfigurable hardware in critical applications like transportation and transaction systems is increasing rapidly. Undetected errors caused e.g. by radiation may result in fatal silent data corruption and unreproducible system crashes. Since it is virtually impossible to build devices which are free from faults, it is essential to embed some sort of fault-tolerance in such devices, which will enable them to work correctly even in the presence of faults. Since the past decade, a lot of research has been done to develop fault-tolerant reconfigurable systems on various granularity levels, although most of them have dealt with the lowest level such as offered by FPGAs.

In [45], we have considered the possibility of implementing low-cost hardware techniques which would allow to tolerate temporary faults in the data-paths of coarse-grained reconfigurable architectures. Our goal was to use less hardware overhead than commonly used duplication or triplication methods. The proposed technique relies on concurrent error detection by using *residue code modulo 3* and re-execution of the last operation, once an error is detected. Simulation results performed for the DART architecture developed at IRISA with all of its data-paths protected using residue code confirmed hardware savings of the proposed approach over duplication.

To cope with the high sensitivity of electronic devices to failures or soft errors, we also proposed a multi-processor system on a dynamically reconfigurable architecture for the design of fault-tolerant systems. First we have proposed and designed a flexible communication model which ensures reliable communication. This work accomplished in the CIFAER project permits to switch from a communication protocol, by reconfiguring the reserved zone for the communication protocol, to a secondary one in order to mitigate communication errors. Some possibilities to integrate this dynamic platform into standardized automotive software infrastructure have also been introduced [62].

In order to exploit the computational power and the flexibility of reconfigurable architectures, and at the same time to guarantee the correct functionality of the entire system, we proposed a fully dynamic MPSoC topology. In this system, all the processors can be dynamically reconfigured, moved or replaced in the system, hence providing fault-tolerant and self-repair capability [61]. A deep exploration of a standard design flow has been done to facilitate the design of this architecture using commercially available FPGAs.

6.1.5. Power Efficient Architectures

6.1.5.1. Coding Techniques Improving Reliability and Power Consumption for On-Chip Buses

Participants: Olivier Sentieys, Sébastien Pillement, Stanislaw Piestrak.

Interconnects are now considered as one of the bottlenecks in the design of system-on-chip (SoC) since they introduce delay and power consumption. To deal with this issue, data coding for interconnect power and timing optimization has been introduced. In today's SoCs these techniques are not efficient anymore due to encoding/decoding circuitry (a codec) complexity or to unrealistic published experimentations. Based on some realistic observations on interconnect delay and power estimation [2], [36], the spatial switching technique [37], [38], [17] is proposed and has been patented. It allows the reduction of delay and power consumption (including extra power consumption due to codecs) for on-chip buses. The concept of the technique is to detect all cross-transitions on adjacent wires and to decide if the adjacent wires are exchanged or not. Results show the spatial switching efficiency for different technologies and bus lengths. The power consumption reduction can reach up to 15% for a 5-mm bus and more if buses are longer and for future CMOS technologies.

Several coding techniques have been suggested to reduce both noise and wire power consumption in on-chip interconnections, like bus-invert coding, low-weight coding, and reduction of the voltage swing of the signal on the wire. Unfortunately, the latter involves reduced noise margin which might result in increased error rate. Recently, Berger-invert code has been suggested to protect communication channels against all asymmetric errors and to decrease power consumption. We have not only shown some inaccuracies of the approach proposed [23], but also suggested a modified encoding scheme and a new design of codec [24]. Implementation results have shown that our approach leads to significant hardware savings and results in reduced error rate and power consumption.

6.1.5.2. Ultra Low-Power Architecture for Control-Oriented Applications in Wireless Sensor Nodes

Participants: Steven Derrien, Adeel Pasha, Olivier Sentieys.

This research work aims at developing ultra low-power SoC for wireless sensor nodes, as an alternative to existing approaches based low-power micro-controllers such as the Texas Instrument's MSP430. The proposed approach tries to reduce the power consumption by using a combination of hardware specialization and power gating techniques. In particular, we use the fact that typical WSN applications are generally modeled as a set of small to medium grain tasks that are implemented on low power microcontroller using light weight *thread*-like OS constructs.

Rather than implementing these tasks in software, we instead propose to map each of these tasks to their own specialized hardware structures that we call a *hardware task*. Such an hardware task consists of a minimalistic (and customized) data-path controlled by a finite state machine (FSM). By customizing each of these hardware implementations to their corresponding task, we expect to significantly reduce the dynamic power dissipated by the whole system. Besides, to circumvent the increase in static power caused by the possibly numerous hardware tasks implemented in the chip, we also propose to combine our approach with *power gating*, so as to supply power to a hardware task only when it needs to be executed. The first results that we obtained are very promising and have led to two publications [60], [59].

The work done in 2009 mainly consisted in providing a system level design flow for specifying these new type of architectures. In particular, we now have a fully automated design flow that can produce a VHDL model of a micro-task starting from a specification in C, using the Gecos compiler infrastructure. We have also started working on a Domain Specific Language (DSL) for specifying the System Level Architecture, and hope to have a fully operational flow by the beginning of 2010.

6.1.6. SoC Modeling and Prototyping on FPGA-based Systems

Participants: François Charot, Kevin Martin, Laurent Perraudeau, Charles Wagner.

CAIRN participates in the SoCLib ANR project (see Section 7.8 for more information) whose goal is to build an open platform for modeling and simulation of multiprocessors system-on-chip (MP-SoC). As part of our participation in this project, we have developed simulation models of the Altera NIOSII processor and of the Altera interconnect (Avalon bus). These models and their associated wrappers now allow NIOSII[4]-based multiprocessor systems to be modeled.

MutekH is a portable operating system developed at LIP6 laboratory. MutekH is a set of libraries built on top of the Hexo exo-kernel. This exo-kernel defines the Hardware Abstraction Layer, providing both portability and support for heterogeneity. This year, as part of our participation to the SocLib project, we have ported Hexo on NIOSII processor based MPSoCs architectures modeled with SoCLib.

In order to validate these different components, a multithreaded version of a H264 video decoding application has been ported on a SoCLib platform composed of several NIOSII processors communicating through the Avalon interconnect structure.

6.2. Compilation and Synthesis for Reconfigurable Platform

Participants: Steven Derrien, Emmanuel Casseau, Daniel Ménard, François Charot, Christophe Wolinski, Olivier Sentieys, Patrice Quinton.

6.2.1. DURASE: Generic Environment for Design and Utilization of Reconfigurable Application-Specific Processors Extensions

Participants: Christophe Wolinski, François Charot, Erwan Raffin, Kevin Martin, Antoine Floch.

This year we focused on the architecture model of an ASIP processor with extended instruction sets. Extended instructions implement identified and selected computational patterns and can be executed sequentially or in parallel with the ASIP core processor instructions. This provides ways to trade execution time against hardware cost.

Our generic simplified architecture is depicted in Figure 4. It is composed of one functionally reconfigurable cell implementing a set of computational patterns (selected by the *DURASE* system [32], [51], [50], [78]) directly connected to the processor data-path. The selected patterns are merged by our merging procedure [69] before synthesis. The cell also contains registers for the case where the generated patterns have more than two inputs and one output (case of the NIOS II). The number of registers and the structure of interconnections are application dependent.

[4]The NiosII processor core is a configurable processor core proposed by Altera. This NiosII processor core is declined in three families (economic, standard, fast). A SoCLib model of the fast version has been previously developed in 2008.

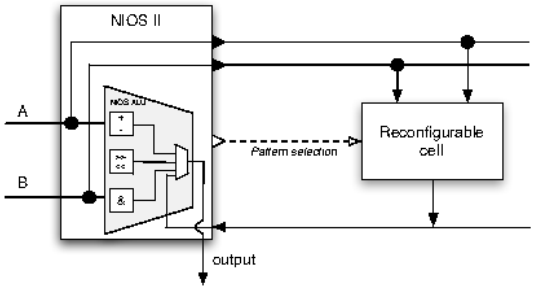

Figure 4. An example of the ASIP "NIOS II" processor with its extension

The *DURASE* system enables automatic synthesis of application specific processor extensions that speed-up application's execution. The system also carries out corresponding source code transformations to match the newly synthesized extensions. Finally, the synthesized extensions are tightly connected to a target processor and used through newly created instructions (see Figure 4 for example of the NIOS II processor and its extension). The design flow adopted in the *DURASE* system is presented in Figure 5. The input to the *DURASE* system is an application code written in C, a target processor instruction set and an architecture model. The output is a processor extension and application specific instructions for accessing this extension. The processor extension is built using a merged pattern implementing all the selected computational patterns. Our system also generates the transformed application source code, including application specific instructions.

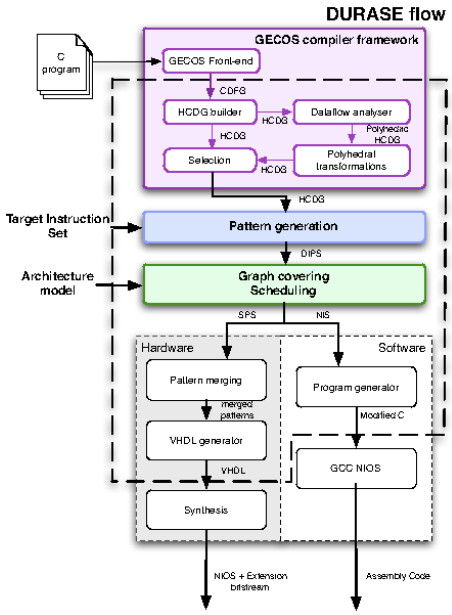

Figure 5. Generic hardware and software extension set generation flow

Our design process involves identification of computational patterns and selection of specific patterns that speed up application execution. The pattern identification and selection are executed in two consecutive steps. In the first step, we explore typical computational patterns and identify the most useful ones for a given application. Our method identifies all computational patterns directly from an application graph satisfying all architectural and technological constraints imposed by target processors and FPGA devices. The considered constraints include a number of inputs and outputs, a number of operators, and a delay of the pattern critical path. Therefore the identified patterns can be well tailored to target processors. The identified computational patterns are then used in the mapping and scheduling step where a subset of patterns is selected for implementation.

The developed *DURASE* system uses advanced technologies, such as algorithms for graph matching and graph merging [69] together with constraints programming methods.

6.2.2. Run-time reconfigurable architecture modeling

Participants: Christophe Wolinski, François Charot, Emmanuel Casseau, Daniel Ménard, Antoine Floch, Erwan Raffin, Steven Derrien.

We have continued to work on the modeling problem of the run-time partially reconfigurable architecture in order to optimize the execution time of the application. The architecture has been defined in the ROMA project. The architecture is parametric, and is composed of memories, a restricted number of communication switches and run time reconfigurable cells at the functional level. This year a new compilation flow has been defined including a meta-model of a generic architecture. The current design flow supports accumulative operators and assures the data flow application's execution. The loop kernel can be mapped on the architecture in such a way that the execution time is minimized.
In the context of the RecMotifs project, we have proposed a specific design flow integrating STMicroelectronics' compiler and our development platform enabling, in the future, the generation of application specific extensions to STMicroelectronics' processors and the compilation of applications on these new architectures. In the first step, a meta-model of the CDFG (Control Data Flow Graph) of ST's compiler was defined. Using model-to-model transformations the resulting graphs obtained by the compiler are transformed into HCDG graphs recognized by our environment. We have used the Kermeta[5] tools for this purpose. Next, we have started to work on the architecture model of the ST processor and its extensions. We have also initialized the work on a new CP (Constraint Programming) model of the scheduler well adapted to the parallel architecture of the entire system composed of the processor, the multi-extensions and the external memory. This model will be used in the future for efficient application compilation.

6.2.3. Architecture-Driven Synthesis of Reconfigurable Cells

Participants: Christophe Wolinski, François Charot, Erwan Raffin.

In the context of the *DURASE* system we have also focused on merging computational patterns to form a corresponding optimized reconfigurable cell. Existing methods cannot control critical paths and placement of multiplexers during merging. This leads to generation of area optimized architectures that often do not satisfy timing constraints. Timing constraints are, however, very important when the clock frequency of an ASIP processor needs to be optimized. Our original approach [69], based on constraint programming, opens a new perspective and enables area optimization of a cell while respecting design constraints. For instance, area minimization of a merged cell without increasing its critical path is possible in our approach. Experiments carried out on MediaBench test suite indicate 50% average reduction of cell area without increasing critical path.

6.2.3.1. Hierarchical Methodology for Floating-Point to Fixed-Point Conversion

Participants: Daniel Ménard, Karthick Parashar, Olivier Sentieys, Romuald Rocher.

[5] http://www.kermeta.org

The problem of converting floating-point algorithms to implementation-friendly fixed-point formats is often solved as an optimization problem where the precision is traded to gain in the implementation cost. The complexity of the problem is known to grow exponentially with more variables for the optimization process. In [58] we propose a *divide and conquer* technique to solve the growing size of the problem. A hierarchical approach has been proposed to perform wordlength optimization of a complete system made-up of several subsystems. At the system level, the fixed-point behavior of each subsystem is modeled by a single noise source located at the subsystem output. The aim is to find the noise power levels of each noise source so as to minimize the implementation cost while maintaining the overall performance. The application performance is evaluated through an original approach mixing simulation and analytical approaches detailed in Section 6.3.1.2. The analytical technique accelerates the simulation of some parts of the system. At the subsystem level, analytical models are used for evaluating the implementation cost and the computation accuracy. Compared to existing approaches, our method allows reducing the optimization time and supporting complex systems by combining the advantages of the simulation and analytical approaches.

6.3. Algorithm Architecture Interaction

Participants: Steven Derrien, Romuald Rocher, Daniel Ménard, François Charot, Christophe Wolinski, Olivier Sentieys, Patrice Quinton.

6.3.1. Computation Accuracy Optimization

Participants: Daniel Ménard, Karthick Parashar, Olivier Sentieys, Romuald Rocher, Hai-Nam Nguyen.

6.3.1.1. Dynamic Precision Scaling

The traditional approach to design a fixed-point system is based on the worst-case principle. For example, for a digital communication receiver, the maximal performance and the maximal input dynamic are retained and the more constraint transmission channel is considered. Nevertheless, the noise and the signal levels evolve during time. Moreover, the data rate depends on the service (video, image, speech) used by the terminal and the required performance (bit error rate) is linked to the service. These various elements show that the fixed-point specification depends on external elements (noise level, input signal dynamic range, quality of service) and can be adapted during time to reduce the average power consumption.

An approach in which the fixed-point specification is adapted dynamically according to the input receiver SNR (Signal-to-Noise Ratio) has been proposed in a concept called *Dynamic Precision Scaling (DPS)*. To adapt the fixed-point specification during time, the architecture integrates flexible operators as presented in Section 6.1.1.

This year, our work on Dynamic Precision Scaling (DPS) has been carried on. This technique allows adapting the fixed-point specification to reduce the power consumption. Our approach interest has been shown on a WCDMA receiver example [57]. A new approach has been proposed to estimate more accurately the data dynamic range [56]. The properties of the application are taken into account to reduce the pessimistic effects of classical analytical approaches like interval arithmetic. The accuracy constraint used in the fixed-point optimization problem is determined from the required application performance. For the bit error rate, the analytical expression of the accuracy constraint according to the bit error rate has been proposed. Our work is now focused on the methodology to find the optimized fixed-point specification. The aim is to find the appropriate optimization algorithm which allows minimizing the implementation cost under accuracy constraint.

6.3.1.2. Fixed-Point Accuracy Evaluation

Analytical techniques have been proposed to accelerate the performance evaluation step, which is the most time consuming step during optimization. The inability to handle all types of operator analytically and the increasing diversity and complexity of signal processing algorithms demand a mixed evaluation approach where both simulation and analytical techniques are used for performance evaluation of the whole system. We also proposed this year to use the spectral density estimate for noise power calculation by having an approximate filter thereby accelerating the process of performance evaluation. We applied this approach to the SSFE (Selective Spanning for Fast Enumeration) algorithm in collaboration with Imec (Interuniversitair Micro-Electronika Centrum), Belgium.

The presence of decision operators has proved to be a serious impediment for a fully analytical noise power estimation technique. We develop a generalized decision operator which can potentially capture the behavior of all possible types of decision operators and provides a fully analytical technique to handle them while performing quantization noise power estimation.

6.3.2. Arithmetic Implementation on GPUs

Participant: Arnaud Tisserand.

6.3.2.1. Arithmetic Library for Cryptography on GPUs

In [44], we present first implementation results on a modular arithmetic library for cryptography on GPUs. Our library, in C++ for CUDA, provides modular arithmetic, finite field arithmetic and some ECC supports. Efficient algorithms and implementations are required for $a \pm b \mod p$, $a \times b \mod p$ where a, b and p are multiple precision integers and p is prime. Those operations are required in finite field arithmetic over $\mathrm{GF}(p)$ and in elliptic curve cryptography (ECC) where sizes are about 200–600 bits. Graphic processor units (GPUs) are used in high-performance computing systems thanks to their massively multithreaded architectures. But due to their specific architecture and programming style, porting libraries to GPUs is not simple even using high-level tools such as CUDA. This work is a part of a software library called PACE [5]. This library is aimed at providing a very large set of mathematical objects, functions and algorithms to facilitate the writing of arithmetic applications.

6.3.2.2. Power Consumption of GPUs

In [35], we investigate how and where the power consumption is located within a GPU board by analyzing the relations between the measured power consumption, the required time and the type of units that are stressed to perform a defined operation. In this paper, we consider Nvidia GPUs used for GPGPU (General Purpose computing using GPU) in a CUDA environment. During the analysis, functional blocks are identified, and their power is characterized using physical measurements. The considered blocks correspond to units that are usually stressed while executing common kernels on the GPU: register file, memory hierarchy and functional units. In addition to the power estimation, our analysis gives us some information on the organization of the memory hierarchy, the behavior of functional units and some undocumented features.

6.3.3. Multi-Antenna Systems

Participants: Olivier Berder, Pascal Scalart, Quoc-Tuong Ngo.

Considering the possibility for the transmitter to get some Channel State Information (CSI) from the receiver, antenna power allocation strategies can be performed thanks to the joined optimization of linear precoder (at the transmitter) and decoder (at the receiver).

A new exact solution of the maximization of the minimum Euclidean distance between received symbols has been proposed for two 16-QAM modulated symbols [54]. This precoder shows an important enhancement of this minimum distance compared to diagonal precoders which leads to a significant BER improvement. This new strategy selects the best precoding matrix among eight different expressions, depending on the value of the channel angle. In order to decrease the complexity, other sets of precoders have been proposed and the performance of the simplest one, composed of only two different precoders, remains very close to the optimal in terms of BER.

An efficient sub-optimal MIMO linear precoder based on the maximization of minimum distance has been proposed for three virtual subchannels [53]. A new virtual MIMO channel representation with two channel angles allows the parameterization of the linear precoder and the optimization of the distance between signal points at the received constellation. As these precoders need a Singular Value Decomposition (SVD) of the propagation channel, an optimized architecture of SVD was proposed for an FPGA implementation [71].

6.3.4. Parallel reconfigurable architectures for LDPC decoding

Participants: Florent Berthelot, François Charot, Charles Wagner, Christophe Wolinski.

LDPC codes are a class of error-correcting code introduced by Gallager with an iterative probability-based decoding algorithm. Their performances combined with their relatively simple decoding algorithm make these codes very attractive for the next satellite and radio digital transmission system generations. LDPC codes were chosen in DVB-S2, 802.11n, 802.16e, 802.3an and CCSDS standards. The major problem is the huge design space composed of many interrelated parameters which enforces drastic design trade-offs. Another important issue is the need for flexibility of the hardware solutions which have to be able to support all the declinations of a given standard.

Previously we have defined a generic architecture template that is composed of several processing modules and a set of interconnection buses for inter-module communications. Each module includes two processing units (called *bitnode* and *checknode* processing units), and a set of memory banks. The number of modules, the number of interconnection buses, the size and the number of memory banks are standard dependent.

This year, we have proposed a generic architecture for a CCSDS LDPC decoder. This architecture uses the regularity and the parallelism of the code and a genericity based on an optimized storage of the data. Two FPGA implementations have been proposed: the first one is low-cost oriented and the second one targets high-speed decoder [39]. Moreover in the context of the RPS2 project, we have designed a parallel architecture suited to the decoding of LDPC for the digital video broadcast DVB-S2 standard. Due the huge codeword length used in the DVB-S2 standard only partly parallel architectures are feasible. The designed architecture exploit the periodicity nature of DVB-S2 LDPC codes.

6.3.5. Algorithm Optimization for Low Energy in Wireless Applications

Participants: Olivier Berder, Tuan-Duc Nguyen, Vinh Tran, Olivier Sentieys.

In wireless distributed networks, where multiple antennas can not be integrated in one node, Cooperative Multi-Input Multi-Output (C-MIMO) techniques help to exploit the space time diversity gain in order to increase performance or to reduce the transmission energy consumption. In [14], strategies using Cooperative MIMO techniques were proposed for Wireless Sensor Network (WSN) where the energy consumption is the most important design criterion. The performance and the energy consumption advantages of Cooperative MIMO technique were investigated, in comparison with the SISO (Single-Input Single-Output), multi-hop SISO and cooperative relay techniques, and an optimal selection of transmit-receive antennas number in terms of energy consumption was also proposed as a function of transmission distances.

Since the wireless nodes are physically separated in cooperative MIMO systems, the imperfect time synchronization between cooperative nodes clocks leads to an unsynchronized MIMO transmission. The performance degradation of this cooperative transmission synchronization error and the cooperative reception additional noise is evaluated by simulations. Two new cooperative reception techniques based on the relay principle and a new efficient space-time combination technique were proposed to increase the energy efficiency of cooperative MIMO systems. Finally, performance and energy consumption comparisons between cooperative MIMO and relay techniques are performed and an association strategy is also proposed to exploit simultaneously the advantages of the two cooperative techniques.
Two MIMO simple and full cooperative relay models are proposed by associating space time codes and cooperative relay. In these two models, a two-antenna source transmits space time codes to two relays and to destination at the same time. The relay nodes use a new Amplify and Forward (AF) protocol and a new Decode and Forward (DF) protocol based on the Alamouti space-time code to forward the signals to destination. The simulations show that a higher performance can be achieved by using these two models in comparison with Alamouti scheme.

6.3.6. Wireless Communications for Automotive Systems

Participants: Olivier Berder, Tuan-Duc Nguyen, Olivier Sentieys, Jérome Astier, Arnaud Carer, Thomas Anger.

The CAPTIV (Cooperative strAtegies for low Power wireless Transmissions between Infrastuctures and Vehicles) project aims at using new radio communications technologies in order to enhance drivers security. In a cooperative network composed of vehicles and road signs equipped with autonomous radio transmitters, the communications can be optimized at different levels. It was shown that space-time codes allow to dramatically decrease the energy consumption of communications between crossroads. In order to both elaborate CAPTIV application program and evaluate the driver behaviour in front of this new kind of information, a specific driving simulator was designed, based on the ECA-FAROS platform. A real prototype has already been evaluated and proves the feasibility of CAPTIV application, and it will be soon optimized thanks to signal processing techniques. If the main goal remains driving assistance, many applications could be implemented on this platform and it will be able to deliver any kind of information (meteo, parking, tourist information, advertisement etc.) [29],[76].

For wireless communications between infrastructure and vehicles, cooperative strategies were defined in order to choose the most energy efficient techniques between cooperative MIMO and relay in the CAPTIV context [55]. The performance of an association of both techniques in terms of Bit Error Rate and energy efficiency was also evaluated and analyzed in [21].

6.3.7. True Random Number Generators

Participants: Renaud Santoro, Olivier Sentieys, Arnaud Tisserand, Philippe Quémerais, Arnaud Carer, Thomas Anger.

The objective of a random number generator (RNG) is to produce random binary numbers which are statistically independent, uniformly distributed and unpredictable. RNGs are necessary in many applications and the number of embedded hardware architectures requiring RNGs is continuously increasing. Generally, a hybrid RNG comprising a True Random Number Generator (TRNG) and a Pseudo Random Number Generator (PRNG) is used. PRNGs are based on deterministic algorithms. They are periodic, and must be initialized by a TRNG. TRNGs are based on a physical noise source (e.g. thermal noise or free running jitter oscillators) and depend strongly on their implementation quality. Most of the TRNGs implemented in FPGA or ASIC use phase jitter produced by a free running oscillator or a Phase-Locked Loop (PLL) [97]. In practice, jitter can be influenced by noise external to the FPGA (power supply noise, temperature) and by chip activity. This dependence is a weakness exploitable by exposing the TRNG in hostile environment conditions [117].

In cryptography, security is usually based on the randomness quality of a key generated by an RNG. Some PRNGs are recognized to produce high quality random numbers [103]. However, their quality depends on TRNG seed randomness. PRNG randomness evaluation is usually performed by using a battery of statistical tests. Several such batteries are reported in the literature including Diehard [106] and NIST [115] batteries. They are all implemented using high-level software programming. When an PRNG is evaluated, designers put a huge bit stream into memory and then submit it to software tests. If the bit stream successfully passes a certain number of statistical tests, the PRNG is said to be sufficiently random. TRNG validation is more complicated as their behavior depends on their construction, on external environments and essentially on a physical noise source which can differ in practice from an ideal noise. However, [100] has described a methodology to evaluate physical generators. The procedure is based on TRNG construction and is the technical reference of the AIS 31 [83]. TRNG weaknesses and external attacks must be prevented on real-time to inhibit TRNG output [117], and a solution is to monitor the TRNG at switch on and during operations by using statistical tests [100], [117].

6.3.7.1. Evaluation of TRNGs under Various Experimental Conditions

Attacking TRNGs is a good solution to decrease the security of a cryptosystem leading to lower security keys or bad padding values for instance. Recently, new TRNGs have been proposed in the literature, however, selecting a robust and efficient TRNG is a difficult problem. To the best of our knowledge, no real and objective comparison of several TRNGs appears in the literature. During this year, we have investigated the randomness behavior, the area and the power consumption of recent TRNGs implemented into FPGA circuits [65]. The randomness of the generator output has been evaluated by using hardware accelerated statistical tests [66].

This year, the possibility to implement the AIS 31 statistical tests in hardware has been studied. Then, the tests have been implemented into ASIC and FPGA targets. The hardware cost shows that the design can be used into low-cost embedded cryptography circuits. Moreover, the data-rate obtained by the designed hardware tests allows to monitor TRNG in real-time.

6.3.7.2. Ochre: a Circuit for On-Chip Randomness Extraction

This year has seen the design and fabrication of an integrated circuit prototype (Ochre) including our architecture proposal for hybrid RNG [15]. The chip is composed of a TRNG based on several free-running ring-oscillators, a cellular-automata-based PRNG and some hardware statistical tests including the FIPS 140-2. The tests monitor the TRNG quality in real time to validate the PRNG seed randomness as proposed in [15], [66]. Ochre has been fabricated in a 130 nm CMOS technology from STMicrocelectronics and is able to reach 800 Mbit/s for 0.3mm^2 and 5mW at 200MHz (see Fig. 6). The circuit has been successfully tested after fabrication. A second version of this chip is currently being designed and will be fabricated in Spring 2010. Ochre V2 will include more stringent statistical tests and also a high-quality PRNG. This chip is intended for quality evaluation of several TRNGs into a VLSI technology.

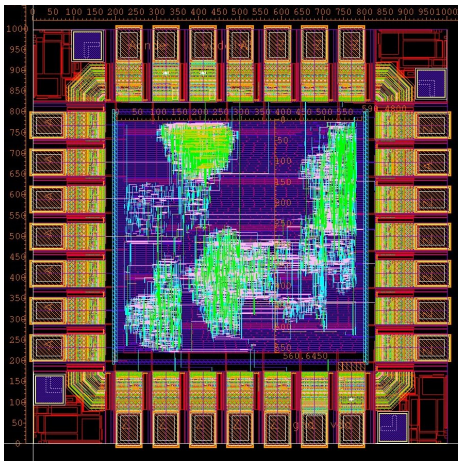

Figure 6. Layout of Ochre Integrated Circuit

6.3.7.3. Arithmetic Operators for Evaluation of TRNG Randomness Quality

In [67], we propose arithmetic operators for the on-the-fly evaluation of TRNG randomness quality. We use the Maurer's universal test included in the NIST and the AIS-31 test-benches. This test requires a large number of arithmetic units and memory banks. So optimization is important for embedded implementations. One of the main task is the evaluation of the Harmonic series for large index values. We use DeTemple-Wang mathematical approximation and polynomial approximations "well-suited" for high-performance hardware implementations. Based on several recent results on computer arithmetic, one can generate very optimized polynomial approximations for one interval. The degree of the polynomial used for an accurate approximation on the whole interval is too high. In this paper, we present a method for splitting the interval into "well-chosen" intervals and one low-degree polynomial per interval. We detail the design and the optimization of the approximation operator. We also present its implementation on FPGAs and the obtained results for on-the-fly evaluation of TRNGs.

6.3.8. Flexible hardware accelerators for biocomputing applications

Participants: Steven Derrien, Naeem Abbas, Patrice Quinton.

It is nowadays acknowledged that FPGA-based hardware acceleration of compute intensive bioinformatics applications is a very viable alternative to cluster (or grid) based approach. One of the issues with this technology is that it remains somewhat difficult to use and to maintain (one is rather designing a circuit rather than programming a machine), and even though there exists several C-to-hardware compilation flows (Mitrion-C, C2H, Gaut, Impulse-C, etc.), they do not offer good enough performance to justify the use of reconfigurable technology. Most successful hardware implementations of bio-computing algorithms were therefore designed by hand at the RTL level by targeting a specific reconfigurable system (if not a specific FPGA technology). Maintaining/upgrading and porting such implementations to other/new systems is therefore a very tedious task, and always comes at the price of a very sensitive performance loss (indeed a complete rewrite is often required). The use of retargetable IP core generators, that are capable of producing an optimized RTL hardware description given a high-level system description of the accelerator, could leverage the use of FPGA and reconfigurable technology for this type of application. Yet there exists such generators for signal processing kernels (FFT, DCT, etc.) and specialized arithmetic functions (mostly floating point), no contribution has been done in the field on biocomputing. This research work, which is part of the ANR BioWiic project, aims at providing a framework for helping semi-automatic generation of flexible IP cores, by widening the scope typical design constraints so as to integrate communication and data reuse optimisations between the host and the hardware accelerator. This research work builds upon the CAIRN research group expertise on automatic parallelization for application specific hardware accelerators. Considered target applications include HMMer, ClustalW and BLAST.

7. Contracts and Grants with Industry

7.1. ITEA2 - GEODES (2008-2011)

Participants: Olivier Sentieys, Olivier Berder, Arnaud Carer, Jérôme Astier, Thomas Anger, Vivek Tovinakere-Dwarakanath, Mahtab Alam.

The GEODES (Global Energy Optimization for Distributed Embedded Systems) project will provide design techniques, embedded software and accompanying tools needed to face the challenge of allowing long power-autonomy of features rich and connected embedded systems, which are becoming pervasive and whose usage is significantly rising. It approaches this challenge by considering all system levels, and notably emphasizes the distributed system view. GEODES is an ITEA2 project which involves partners from France, Austria, Italy and the Netherlands: Thales (FR, IT, NL), Sensaris (FR), CNRS (LEAT and IRISA) (FR), CETMEF/MARTEC (FR), Infineon (AU), Thomson (FR), TUV (AU), UAQ (IT), Phillips (NL), Organo (AU), TI-WMC (NL). In GEODES Cairn will provide to partners the PowWow very power sensor platform including reconfigurable hardware accelerators. CAIRN will also contribute on link and MAC layers strategies to a global optimization of the energy, and define and optimize advanced signal processing, error detection and correction and medium access (MAC) techniques in order to reduce the transmit power as well as the useless listening of the communication media. In particular, the case of cooperative strategies like cooperative MIMO or relaying techniques will be investigated.

7.2. NANO2012 Program - S2S4HLS (2008-2012)

Participants: Emmanuel Casseau, Steven Derrien, Daniel Ménard, Olivier Sentieys, Loïc Cloatre, Amit Kumar, Antoine Morvan, Chenglong Xiao, Jean-Charles Naud.

High-level synthesis (HLS) tools start to be used for industrial designs. HLS is analogous to software compilation transposed to the hardware domain. From an algorithmic behavior of the specification, HLS tools automate the design process and generate a register transfer level RTL architecture taking account of user-specified constraints. However, design performance still depends on designer's skill to write the appropriate source code. The S2S4HLS (Source-to-Source for High-Level Synthesis) project intends to process source code transformations to guide synthesis hence leading to more efficient designs, and aims at providing a toolbox for automatic C code source-to-source transformations. The project is focused on

three complementary goals to push the limits of existing HLS tools: loop transformations for performance optimization and a better resource usage, automatic floating-point to fixed-point conversion and synthesis of multi-mode architectures. S2S4HLS is organized into three sub-projects targeting these three objectives. The project is in close collaboration with ST Microelectronics and Compsys team at Inria Rhône-Alpes, within the overall INRIA-ST partnership agreement. It is financed by the Ministry of Industry in the Nano2012 program. Cairn is responsible of the project and involved in the three workpackages.

7.3. NANO2012 Program - RecMotifs (2008-2012)

Participants: François Charot, Antoine Floch, Jérémie Guidoux, Christophe Wolinski.

The RecMotifs project aims at the generation of application specific extensions targeting the STxP70 processor from STMicroelectronics. Cairn will study advanced technologies algorithms for graph matching and graph merging together with constraints programming methods. The project is in close collaboration with ST Microelectronics within the overall INRIA-ST partnership agreement. It is financed by the Ministry of Industry in the Nano2012 program.

7.4. ANR Architectures du Futur Open-People (2009-2011)

Participants: Daniel Chillet, Robin Bonamy, Olivier Sentieys.

The Open-People (Open Power and Energy Optimization PLatform and Estimator) project aims at defining a complete platform for low power estimation and optimization. The platform will be composed of hardware boards to support measurements for the applications. End-users will be able to upload their applications through a web portal, and to control the power measurements of the execution of their applications on a specific electronic board. The Open-People project will also propose a complete power component model library which allows end-users to estimate the power consumption of some parts of the applications without making measurements. This will allow to quickly evaluate the different design choices regarding the power consumption. Finally, through the web portal http://www.open-people.org, Open-People will propose software tools to apply power optimizations. In this project, CAIRN team will develop power model for FPGA components using dynamic reconfiguration. Open-People involves LabSticc (Lorient), Trio (Nancy), CAIRN (Rennes/Lannion) and Dart (Lille/Valenciennes) teams from Inria, Leat at Nice, Thales (Colombes) and InPixal (Rennes).

7.5. ANR BioWiiC (2009-2011)

Participants: Steven Derrien, Naeem Abbas, Patrice Quinton.

The increasing flow of genomic data provided by the steadily improvement of new biotechnologies cannot be now efficiently exploited without a systematic *in silico* analysis. Data need to be filtered, curated, classified, annotated, validated, etc., to be actively used in a discovery process. The design of such complex pipeline of processing stages is known to be an extremely tedious task as their designers have to deal with both specification and implementation issues. Indeed, the execution time of such *workflows* is very often a bottleneck as huge amount of data has to be processed. Therefore, the goal of the BioWiiC (Bioinformatics Workflows for Intensive Computation) project is twofold:

- Reducing the design time of complex bioinformatics pipelines by providing a domain specific workflow environment;
- Reducing the execution time of these workflows through the use of parallel execution on GPU, FGPA and clusters of PC whenever possible.

The ANR BioWiic project is funded for 3 years, and involves several institutions (INRA-MIG, Ouest Genopole, CAIRN and Symbiose project-teams at INRIA) and Universities (Eliaus Laboratory at Université de Perpignan). For more details see http://biowic.inria.fr. CAIRN will provide a framework for helping semi-automatic generation of flexible IP cores, by widening the scope typical design constraints so as to integrate communication and data reuse optimizations between the host and the hardware accelerator.

7.6. ANR Architectures du Futur - CIFAER (2008-2011)

Participants: Sébastien Pillement, Manh Pham, Olivier Sentieys, Samuel Mouget.

In various application domains, emerging requirements lead to the definition of new architectures for electronic embedded systems. In the automotive context, investigated solutions correspond to network of processing elements, distributed in the vehicle. In this context, the research activity considered in the CIFAER (Flexible Intra-Vehicule Communications and Embedded Reconfigurable Architectures) project is the definition of an innovative embedded architecture, based on general purpose processor with reconfigurable processing areas and on the use of adaptable interfaces (radio and powerline communications). Efficient software layers in the associated operating system will be investigated to enable new services as dynamic reconfiguration and task migration for error tolerance. CIFAER involves Irisa, IETR Rennes, Ireena Nantes, Atmel and Geensys. CAIRN will propose and develop the dynamically reconfigurable platform used a the test vehicle of the project. This platform will include fault-tolerant mechanisms for error mitigation.

7.7. ANR Architectures du Futur - FOSFOR (2008-2011)

Participants: Daniel Chillet, Sébastien Pillement, Manh Pham, Ludovic Devaux, Didier Demigny.

The Fosfor (Flexible Operating System FOr Reconfigurable platform) project aims at reconsidering the structure of the RTOS which is generally implemented in software, centralized, and static, by proposing a distributed RTOS with homogeneous interface from the application point of view. We propose to exploit dynamic and partial reconfiguration of the reconfigurable SoC. In this context, the tasks are statically or dynamically deployed (i.e. instantiated) on software units (general processors) or hardware units (reconfigurable areas). Flexibility of the OS will be achieved thanks to virtualization mechanisms of OS services, such that the tasks of the application are executed and communicate without prior knowledge of their assignment to software or hardware. FOSFOR involves Irisa, LEAT Nice, ETIS Cergy, Xilinx and Thales. CAIRN will propose and include in the FOSFOR OS a flexible communication infrastructure and its control management.

7.8. ANR Technologies Logicielles - SoCLib (2007-2010)

Participants: François Charot, Kevin Martin, Laurent Perraudeau, Charles Wagner.

The aim of SocLib (An Open Modeling and Simulation Platform for System-on-Chip Design) is to build an open platform for modeling and simulation of multi-processors system-on-chip, that can be used by both universities and industrial companies. The core of the platform is a library of simulation models for virtual components (IP cores), with a guaranteed path to silicon. The main concern of the SocLib project is a true interoperability between the IP cores: all SocLib components are written in SystemC and respect the VCI (Virtual Component Interface standard) communication protocol. CABA (cycle-accurate and bit-accurate) and TLMT (transaction level model with time) simulation models are proposed. For more details see http://soclib.lip6.fr.

7.9. Pôle Images et Réseaux - SPRING (2008-2009)

Participants: Renaud Santoro, Thomas Anger, Arnaud Carer, Olivier Sentieys.

The aim of the Spring (Shelf Proof Random Integrated Number Generator) project is the design of high-performance and high-rate Quasi-True Random Number Generators. Randomness comes from the random jitter of clock generators in last FPGAs or SoCs. The main contribution is the capacity of the system to measure in real-time the jitter and to characterize the randomness quality using hardware accelerated statistic tests. Spring involves a close collaboration with a company specialized in security for which CAIRN will provide an IP of high-quality high-rate and self-tested TRNG.

7.10. Pôle Images et Réseaux - Transmedi@ (2008-2009)

Participants: Olivier Sentieys, Emmanuel Casseau, Daniel Chillet, Cécile Beaumin-Palud, Arnaud Carer, Thomas Anger.

The TransMedi@ project addresses the issue of video transcoding, and more generally media processing, with very-high performance for network infrastructures and high quality for broadcast equipments. The aim of Transmedi@ is to propose flexible reconfigurable co-processing architectures for the acceleration of video algorithms. In the context of network infrastructure, the platform has to be able to transcode in real time several video streams from various video formats and norms, while in the context of broadcast the main constraint comes from the high-quality (HD) of the video. CAIRN is involved in the definition of this platform and will propose innovating structures for reconfigurable coarse-grain processing and data transfer and storage, in this context of video processing. TransMedi@ involves a close collaboration with Alcatel, Envivio, Telecom Bretagne and IETR/Supelec. For more details see http://transmedia.irisa.fr.

7.11. Pôle Images et Réseaux - RPS2 (2008-2010)

Participants: Florent Berthelot, François Charot, Charles Wagner, Christophe Wolinski.

The RPS2 project started in November 2008. It aims at developing a FPGA-based demonstrator of a DVB-S2 receiver targeting professional applications. RPS2 involves three partners: Inria Rennes, Ditocom and Supelec Rennes. The contribution of CAIRN concerns the design of the hardware architecture of the FEC (Forward Error Correction) process of the DVB-S2 decoding system. This hardware architecture implements low-density parity-check (LDPC) code decoding.

7.12. ANR Architectures du Futur - ROMA: Reconfigurable Operators for Multimedia Applications (2007-2010)

Participants: Emmanuel Casseau, Antoine Floch, Shafqat Khan, Daniel Ménard, François Charot, Christophe Wolinski, Erwan Raffin, Olivier Sentieys.

ROMA is an ANR "architectures du futur" project which involves IRISA-CAIRN, CEA-LIST, CNRS-LIRMM and Thomson R&D France. The ROMA project proposes to develop both a design methodology and a reconfigurable processor able to adapt its computing structure to video and image processing applications. The processor is built around a pipeline of coarse grain reconfigurable operators exhibiting efficient power and performance features. Flexibility is obtained through the use of mutable units. These units can be configured for the implemented function, the number representation of the data and the data bit-width. The configuration of the processor is dynamically done all along the application depending on the tasks that are to be carried out. Higher performance in terms of power consumption and computing power, with at least one-magnitude order with regards to state-of-the-art energy-efficient reconfigurable architectures, is expected. CAIRN is the leader of this project. For more details see http://roma.irisa.fr.

7.13. OverSoc (2005-2009)

Participants: Daniel Chillet, Sébastien Pillement.

The main goal of the ANR OverSoc project is to develop a global exploration and evaluation methodology to design and validate a Reconfigurable SoC (RSoc) platform managed by an embedded RTOS. Also, the OveRSoC project aims at providing SoC designers with a framework for choosing the right RTOS services architecture according to a particular RSoC platform. The main result of this project is the DOGME tool which includes all the partner developments and supports the OverSoC methodology. This tool proposes a library of operating system services that can be easily completed to support specific OS functionality. The tool supports the SystemC generation of the platform and guides the designer through different design choices (architecture, operating system, application characteristics). Several examples of platform explorations have been issued to illustrate the tool and methodology capabilities. OverSoc involves Etis (Cergy) and LIP6 (Paris).

7.14. Captiv (2006-2009)

Participants: Olivier Berder, Tuan-Duc Nguyen, Jérome Astier, Olivier Sentieys.

The CAPTIV (Cooperative strAtegies for low Power wireless Transmissions between Infrastuctures and Vehicles) project is granted by the Brittany Region and involves Telecom Bretagne and IETR. The scientific objective of this research program is the study and the realization of communication systems between vehicles and road infrastructure (e.g. signs traffic) at low cost and at low-energy consumption. For more details see http://captiv.irisa.fr.

8. Other Grants and Activities

8.1. National Initiatives

The CAIRN team has currently some collaboration with the following laboratories: CEA List, SATIE ENS Cachan, LEAT Nice, Lab-Sticc (Lorient, Brest), LIRMM Montpellier, ELIAUS Perpignan, ETIS Cergy, LIP6 Paris, IETR Rennes, Ireena Nantes; and with the following INRIA project-teams: Pops, Arénaire, Ares, Compsys, Espresso, Symbiose, TexMex.

8.1.1. Research Organization of CNRS (GDR)

The team participates in the activities of:

- GdR SOC-SIP (*System On Chip & System In Package*), working groups on reconfigurable architectures, embedded software for SoC, low power issues. See http://www.lirmm.fr/soc_sip/. CAIRN is the leader of the group on reconfigurable architectures.
- GdR ISIS (*Information Signal ImageS*), working group on *Algorithms Architectures Adequation*.
- GdR ASR (*Architectures Systèmes et Réseaux*)
- GdR IM (*Informatique Mathématique*), C2 working group on Codes and Cryptography

8.1.2. PEPS CNRS FiltrOptim with ENS Lyon/LIP

Participants: Olivier Sentieys, Daniel Ménard, Thibault Hilaire, Romuald Rocher, Pascal Scalart.

Efficient and robust signal processing: optimization of digital filter synthesis in fixed-point and floating-point arithmetic.

8.1.3. PEPS CNRS with ENS Cachan/SATIE

Participants: Olivier Sentieys, Olivier Berder, Patrice Quinton.

Energy scavenging and power software management in the human environment

8.2. European Initiatives

The CAIRN team members are involved in close international cooperations with the following laboratories and universities:

- Imec (Belgium) on scenario-based fixed-point data format refinement to enable energy-scalable of Software Defined Radios (SDR);
- University of Erlangen-Nuremberg and Dresden University of Technology (Germany) on massively parallel embedded reconfigurable architectures and on dynamic reconfiguration optimisation in the mesh fabric;
- Lund University (Sweden) on constraints programming approach application in the reconfigurable data-paths synthesis flow;
- Computer Vision and Robotic Group of the Institute for Informatics and Applications at the University of Girona (Spain) on parallel architectures for vision algorithms applied to underwater robot;
- University of Eindhoven (Netherlands) on reconfigurable data-path synthesis;
- University of Leiden (Netherlands) on parallel architecture synthesis;
- Code and Cryptography group of University College Cork (Ireland) on arithmetic operators for cryptography.

8.3. International Initiatives

The CAIRN team members are involved in close international cooperations with the following laboratories and universities:

- LRTS laboratory of Laval University in Québec (Canada) on architectures for MIMO systems, with funds from FFQR and INRIA "Associated Team" (2006-2008);
- LSSI laboratory of Québec University in Trois-Rivières (Canada) on the design of architectures for digital filters and mobile communications;
- ENIT (Tunisia) on architectures for mobile communications;
- Computer Science Department of the University of Colorado State in Fort-Collins (USA) on loop parallelization and on the development of high-level synthesis tools;
- Los Alamos National Laboratory (USA) on optimized application specific reconfigurable architectures design;
- University of Adelaide (Australia) on arithmetic operators;
- University of Queensland (Australia) on reconfigurable architectures for scientific processing;
- University of California, Riverside (USA) on optimized image processing applications synthesis;
- VLSI CAD lab of the Electrical and Computer Engineering Department of University of Massachusetts at Amherst, USA on CAD tools for arithmetic datapath synthesis and optimization;
- University of Douala, University of Yaoundé and University of Dschang in Cameroun on models and tools for parallelization. This cooperation takes place in the scope of the SARIMA GIS for the development of research laboratories in Mathematics and Computer Science in Africa.

8.4. Exterior research visitors

- Sébastien Roy (Laval University, Canada) from June for 6 weeks.
- Michel Thériault (Laval University, Canada) from May for 4 months.
- Carole Thon-Adjallin (Laval University, Canada) from May for 4 months.
- Liam Marnane (University College Cork, Ireland) for one week in March.
- Daniel Gomez-Prado (University of Massachussets, Amherst, USA) for one week in January.
- Maceij Ciesielsky (University of Massachussets, Amherst, USA) for one week in June.

9. Dissemination

9.1. Scientific Community Animation

F. Charot, O. Sentieys and A. Tisserand are members of the steering committee of a spring school for graduate students on embedded systems architectures and associated design tools (ARCHI), organized under the auspices of the CNRS.

S. Pillement, O. Sentieys and A. Tisserand organized the ARCHI'09 *école thématique sur les architectures des systèmes matériels enfouis et méthodes de conception associées* in Pleumeur-Bodou, March 30th – April 3rd 2009. Details on http://www.irisa.fr/archi09/.

S. Pillement is a member of the Program Committee of IEEE FPL, SPL, DTIS and ERSA.

P. Quinton is member of the steering committee of the System Architecture MOdelling and Simulation (SAMOS) workshop and a member of the scientific committee of ASAP.

O. Sentieys is a member of the steering committee of the SOC-SIP Expert Group at the CNRS and of the GDR SOC-SIP. He is the chair of the IEEE Circuits and Systems (CAS) French Chapter.

O. Sentieys was a member of the organizing committee of COGIST'09.

O. Sentieys was a member of technical program committee of the following conferences: IEEE DDECS, IEEE ISQED, IEEE VTC, IEEE DDECS, DCIS, DTIS, SBCCI, FTFC, GRETSI, Sympa. He is on the editorial board of Journal of Low Power Electronics, American Scientific Publishers.

A. Tisserand was a member of technical program committee of the following conferences: IEEE ARITH 19, FTFC and SympA. He is a member of the editorial board of the International Journal of High Performance Systems Architecture, Inderscience.

C. Wolinski was a member of technical committee of the following conferences: IEEE/ACM DATE, IEEE FPL, Euromicro DSD, IEEE ISQED, SympA. He is a member of Board of Directors of Euromicro Society.

9.2. Current Ph.D. Subjects

- Naeem Abbas, Flexible Hardware Accelerators for Biocomputing Applications
- Mahtab Alam, Power Aware Signal Processing for Reconfigurable Radios in the context of Wireless Sensor Networks
- Andrei Banciu, New Digital Design Methodology for Multi Giga bits/s Tranceivers
- Robin Bonamy, Power Consumption Modelling and Optimisation for Reconfigurable Platform
- Thomas Chabrier, Reconfigurable Arithmetic Units for Cryptoprocessors with Protection against Side Channel Attacks.
- Antoine Eiche, Real-Time Scheduling for Heterogeneous and Reconfigurable Architectures using Neural Network Structures
- Ludovic Devaux, Flexible Interconnect Infrastructure for Dynamically Reconfigurable Architecture
- Antoine Floch, Pattern Recognition for Processor Instruction-Set Extension
- Erwan Grace, Memory-Oriented Reconfigurable Embedded Architecture
- Shafqat Khan, Flexible Operators with Sub-Word Parallelism for Multimedia Applications
- Kevin Martin, Extended Instruction-Set Generation for Processors Embedded in an FPGA
- Antoine Morvan, Loop Transformations for Design Space Exploration in High-Level Synthesis
- Jean-Charles Naud, Source-to-Source Code Transformation for Fixed-Point Conversion
- Quoc-Tuong Ngo, Optimization of Precoding Strategies for Multi-User MIMO-OFDM Systems
- Hai-Nam Nguyen, Dynamic Precision Scaling for Mobile Communications
- Cécile Beaumin-Palud, Reconfigurable Architecture for High-Performance Video Transcoding
- Karthick Parashar, System-level Approach for Implementation and Optimization of Signal Processing Applications into Fixed-Point Architectures
- Danuta Pamula, Arithmetic Operators for Cryptography.
- Adeel Pasha, A Reconfigurable SoC with Very Low Energy Consumption Adapted for the Domain of Wireless Communicating Objects
- Manh Pham, Embedded Computing Architecture with Dynamic Hardware Reconfiguration for Intelligent Automotive Systems
- Erwan Raffin, Run-time Reconfigurable Systems: Compilation and Synthesis Aspects
- Matthieu Texier, Low-Power Embedded Multi-Core Architectures for Mobile Systems
- Michel Theriault, Transmit Beam-forming for Distributed Wireless Access with Centralized Signal Processing
- Vivek Tovinakere-Dwarakanath, Ultra-Low Power Reconfigurable Controllers for Wireless Sensor Networks

- Le Quang Vinh Tran, Energy Optimisation of Cooperative Transmissions for Wireless Sensor Networks
- Chenglong Xiao, Pattern-Based Guided High-Level Synthesis

9.3. Seminars and Invitations

O. Berder gave a talk on *CAPTIV : Consommation et strAtégies cooPératives pour les Transmissions entre infrastructures et Véhicules* at the *Congrès international ATEC - ITS France*, Versailles, France, in February 2009.

O. Sentieys gave a talk on *Energy-efficient HW/SW techniques for Wireless Sensor Networks* at the workshop "Co-conception matériel/logiciel orientée basse consommation" of the GdR SoC-SiP, Lyon, in March 2009.

O. Sentieys gave a talk at the National Workshop of the GdR SoC-SiP (System-On-Chip & System-In-Package), Paris on *Some challenges and opportunities for energy reduction in Wireless Sensor Networks* in June 2009.

A. Tisserand gave an invited talk at the conference FTFC 2009 (*Faible Tension, Faible Consommation*), Neuchâtel, Switzerland on *Low-Power Arithmetic Operators* (see [30]).

A. Tisserand gave an invited talk at RAIM 2009 (*Rencontres Arithmétiques de l'Informatique Mathématique*), Lyon, France on *Secured Arithmetic Operators in Cryptography*.

A. Tisserand gave an invited talk at the seminar of the Electrical and Computer Engineering Department, University of Massachusetts, Amherst, U.S.A. on *Secured Arithmetic Operators in Cryptography*.

O. Sentieys gave a talk at the Inria/DGA seminar on telecommunications on *Architectures and Tools for the Design of Reconfigurable Radio Systems*.

T. Anger and O. Sentieys demonstrated PowWow platform for Wireless Sensor Networks at the ITEA Symposium, Madrid, in October 2009.

E. Casseau gave a lecture at ARCHI09 on sub-word parallelism in April 2009.

O. Sentieys gave a lecture at ARCHI09 on on-chip interconnect technology and architecture in April 2009.

A. Tisserand gave a lecture at ARCHI09 on secured arithmetic operators in April 2009.

Christophe Wolinski presented an invited paper on *How constraints programming can help you in the generation of optimized application specific reconfigurable processor extensions* at ERSA 2009, Las Vegas, USA (see [32]).

C. Wolinski gave an invited talk on *Design and Utilization of Reconfigurable Application-Specific Processors Extensions* at the Lawrence Livermore National Laboratory, USA.

C. Wolinski gave an invited talk on *DURASE: Generic Environment for Design and Utilization of Reconfigurable Application-Specific Processors Extensions* at Space Data Systems, Los Alamos National Laboratory, USA .

K. Martin, Ch. Wolinski, F. Charot, A. Floch presented *DURASE : Generic Environment for Design and Utilization of Reconfigurable Application-Specific Processors Extensions* at the DATE University Booth, Nice, France in April 2009.

F. Charot participated to the presentation of the SoCLib project at the DATE 2009 Exhibition Forum in April 2009 and at the *Journée thématique Image et Systèmes Embarqués*, Supelec, Rennes in May 2009.

9.4. Teaching and Responsabilities

There is a strong teaching activity in the CAIRN team since most of the permanent members are Professors or Associate Professors.

P. Quinton is the deputy-director of Ecole Normale Supérieure de Cachan, responsible of the Brittany branch of this school.
E. Casseau is the Director of Academic Studies of ENSSAT since Sep. 2009.
C. Wolinski is the Director of Academic Studies of ESIR since May 2009.
P. Scalart is the Head of the Electronics Engineering department of ENSSAT.
O. Sentieys is responsible of the "Embedded Systems" branch of the SISEA Master of Research (M2R).

P. Quinton, L. Perraudeau, S. Pillement, D. Chillet and C. Wolinski serve in the hiring committee of University of Rennes 1.
S. Pillement serves in the hiring committee of University of Cergy.
O. Sentieys serves in the hiring committee of INSA Rennes and UBS Lorient.

O. Berder's main teaching activities at ENSSAT are *signal processing*, *microprocessor architecture*, and *wireless communications*. He also teaches *signal processing* at IUT Lannion and *mobile communications* at ENI Gabès, Tunisia.
D. Chillet teaches a course on *advanced processors architectures* in M2R/ENSSAT and on *Low-power digital CMOS circuits* at Telecom Bretagne.
E. Casseau's main teaching activities are *signal processing* and *hardware description language*. He also teaches *Soc design methodologies* at Telecom Bretagne Engineering school and *Hardware design language* in Master Microelectronics System Design and Technology at ENSICAEN.
S. Pillement teaches at IUT Lannion. He also teaches a course on Network on Chip in the Master SIC at ENI Sousse, Tunsia.
R. Rocher teaches at IUT Lannion.
P. Quinton teaches at ENS Cachan, IFSIC and M2R.
P. Scalart teaches courses on signal processing at ENSSAT.
O. Sentieys teaches at ENSSAT and M2R where he gives courses on *Methodologies for integrated system design* and signal processing. He also teaches *Digital IC: from synthesis to implementation* in the Master Microelectronics System Design and Technology at ENSICAEN.
C.Wolinski is responsible for the following courses: Design of Embedded Systems, Signal, Image, Architectures, Advanced Architectures.

ENSSAT stands for "Ecole Nationale Supérieure des Sciences Appliquées et de Technologie" and is an "Ecole d'Ingénieurs" of the University of Rennes 1, located in Lannion.
Ifsic stands for "Institut de Formation Supérieure en Informatique et Communication".
ESIR (formerly DIIC) stands for "École supérieure d'ingénieur de Rennes" and is an "Ecole d'Ingénieurs" of the University of Rennes 1, located in Rennes.
M2R stands for Master of Research, second year.

10. Bibliography

Major publications by the team in recent years

[1] L. COLLIN, O. BERDER, P. ROSTAING, G. BUREL. *Optimal Minimum Distance Based Precoder for MIMO Spatial Multiplexing Systems*, in "IEEE Transactions on Signal Processing", vol. 52, n^{o} 3, March 2004.

[2] A. COURTAY, O. SENTIEYS, J. LAURENT, N. JULIEN. *High-level Interconnect Delay and Power Estimation*, in "Journal of Low Power Electronics (JOLPE)", vol. 4, n^{o} 1, 2008, p. 21-33.

[3] R. DAVID, S. PILLEMENT, O. SENTIEYS. *Energy-Efficient Reconfigurable Processssors*, in "Low Power Electronics Design", C. PIGUET (editor), Computer Engineering, Vol 1, chap. 20, CRC Press, August 2004.

[4] S. DERRIEN, P. QUINTON. *Parallelizing HMMER for Hardware Acceleration on FPGAs*, in "18th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2007), Montreal, Canada", July 2007, p. 10–18, Best Paper Award.

[5] L. IMBERT, A. PEIRERA, A. TISSERAND. *A Library for Prototyping the Computer Arithmetic Level in Elliptic Curve Cryptography*, in "Proc. Advanced Signal Processing Algorithms, Architectures and Implementations XVII", F. T. LUK (editor), vol. 6697, n^{o} 66970N, SPIE, San Diego, California, U.S.A., August 2007, p. 1–9, http://dx.doi.org/10.1117/12.733652.

[6] K. KUCHCINSKI, C. WOLINSKI. *Global Approach to Scheduling Complex Behaviors based on Hierarchical Conditional Dependency Graphs and Constraint Programming*, in "Journal of Systems Architecture", vol. 49, n^{o} 12-15, December 2003.

[7] D. MENARD, D. CHILLET, O. SENTIEYS. *Floating-to-fixed-point Conversion for Digital Signal Processors*, in "EURASIP Journal on Applied Signal Processing (JASP), Special Issue Design Methods for DSP Systems", vol. 2006, n^{o} 1, 2006, p. 1–15.

[8] D. MENARD, O. SENTIEYS. *Automatic Evaluation of the Accuracy of Fixed-point Algorithms*, in "IEEE/ACM Design, Automation and Test in Europe (DATE-02), Paris", March 2002.

[9] S. PILLEMENT, O. SENTIEYS, R. DAVID. *DART: A Functional-Level Reconfigurable Architecture for High Energy Efficiency*, in "EURASIP Journal on Embedded Systems (JES)", 2008, p. 1-13, Article ID 562326, 13 pages.

[10] C. PLAPOUS, C. MARRO, P. SCALART. *Improved signal-to-noise ratio estimation for speech enhancement*, in "IEEE Transactions on Speech and Audio Processing", vol. 14, n^{o} 6, 2006.

[11] A. TISSERAND. *High-Performance Hardware Operators for Polynomial Evaluation*, in "Int. J. High Performance Systems Architecture", vol. 1, n^{o} 1, March 2007, p. 14–23, http://dx.doi.org/10.1504/IJHPSA.2007.013288, invited paper.

[12] C. WOLINSKI, M. GOKHALE, K. MCCABE. *Polymorphous fabric-based systems: Model, tools, applications*, in "Journal of Systems Architecture", vol. 49, n^{o} 4-6, September 2003.

Year Publications

Doctoral Dissertations and Habilitation Theses

[13] F. B. ABDALLAH. *Étude et optimisation de l'interaction processeurs-architectures reconfigurables dynamiquement, Study and optimisation of dynamically reconfigurable architectures - processors interaction*, University of Rennes 1, ENSSAT and University of Tunis, ENIT, October 2009, Ph. D. Thesis.

[14] T.-D. NGUYEN. *Cooperative MIMO Strategies for Energy Constrained Wireless Sensor Networks*, University of Rennes 1, ENSSAT, May 2009, Ph. D. Thesis.

[15] R. SANTORO. *Vers des générateurs de nombres aléatoires uniformes et gaussiens à très haut débit, Towards High-Rate Uniform and Gaussian Random Number Generators*, University of Rennes 1, ENSSAT and Laval University, Québec, CA, December 2009, Ph. D. Thesis.

Articles in International Peer-Reviewed Journal

[16] D. CHILLET, S. PILLEMENT, O. SENTIEYS. *Real-Time Scheduling on Heterogeneous SoC Architectures Using Inhibitor Neurons in a Neural Network*, in "Journal of Systems Architecture", 2009, Submitted.

[17] A. COURTAY, J. LAURENT, O. SENTIEYS. *Spatial Switching data coding technique analysis and improvements for interconnect power consumption optimization*, in "Journal of Low Power Electronics (JOLPE)", 2009, Submitted.

[18] L. DEVAUX, S. B. SASSI, S. PILLEMENT, D. CHILLET, D. DEMIGNY. *Flexible interconnection network for dynamically and partially reconfigurable architectures*, in "International Journal on Reconfigurable Computing (IJRC)", 2010, to appear.

[19] J. LALLET, S. PILLEMENT, O. SENTIEYS. *Efficient and Flexible Dynamic Reconfiguration for Multi-Context Architectures*, in "Journal of Integrated Circuits and Systems", vol. 4, n^{o} 1, 2009, p. 36-44.

[20] B. MIRAMOND, E. HUCK, F. VERDIER, A. BENKHELIFA, B. GRANADO, M. AICHOUCH, J. C. PREVOTET, D. CHILLET, S. PILLEMENT. *OveRSoC : a Framework for the Exploration of RTOS for RSoC Platforms*, in "International Journal of Reconfigurable Computing", 2009, Submitted.

[21] T. NGUYEN, O. BERDER, O. SENTIEYS. *Energy efficient cooperative strategies for infrastructure to vehicle communications*, in "IEEE Transactions on Intelligent Transportation Systems", 2010, Submitted.

[22] S. PIESTRAK. *A note on RNS architectures for the implementation of the diagonal function*, in "Information Processing Letters", 2009, Submitted.

[23] S. PIESTRAK, S. PILLEMENT, O. SENTIEYS. *Comments on 'A low-power dependable Berger code for fully asymmetric communication'*, in "IEEE Communications Letters", 2009, Submitted.

[24] S. PIESTRAK, S. PILLEMENT, O. SENTIEYS. *On designing efficient codecs for bus-invert Berger code for fully asymmetric communication*, in "IEEE Transactions on Circuits and Systems II", 2009, Submitted.

[25] S. PILLEMENT, J. PHILIPPE, O. SENTIEYS. *Spatio-temporal Coding to Improve Speed and Noise Tolerance of On-chip Interconnect*, in "MicroElectronics Journal", 2010, to appear.

[26] R. ROCHER, D. MENARD, O. SENTIEYS, P. SCALART. *Accuracy Evaluation of Fixed-Point based LMS Algorithm*, in "Digital Signal Processing", 2010, to appear.

[27] C. WOLINSKI, K. KUCHCINSKI, E. RAFFIN. *Automatic Design of Application-Specific Reconfigurable Processor Extensions with UPaK Synthesis Kernel*, in "ACM Transactions on Design Automation of Electronic Systems", 2010, to appear.

Articles in National Peer-Reviewed Journal

[28] D. CHILLET, S. PILLEMENT, O. SENTIEYS. *Ordonnancement de tâches par réseaux de neurones pour architectures de SoC hétérogènes*, in "Traitement du signal", vol. 26, n^{o} 1, 2009, p. 77-89.

Invited Conferences

[29] O. BERDER. *CAPTIV : Consommation et strAtégies cooPératives pour les Transmissions entre infrastructures et Véhicules*, in "Congrès international ATEC - ITS France, Versailles, France", February 2009.

[30] A. TISSERAND. *Low-Power Arithmetic Operators*, in "Proc. of the 8ème journées d'études Faible Tension Faible Consommation, Neuchâtel, Switzerland", June 2009.

[31] A. TISSERAND. *Opérateurs arithm'etiques sécurisés*, in "3ème Rencontres Arithmétique de l'Informatique Mathématique (RAIM)", October 2009.

[32] C. WOLINSKI, K. KUCHCINSKI, K. MARTIN, R. RAFFIN, F. CHAROT. *How constraints programming can help you in the generation of optimized application specific reconfigurable processor extension*, in "Proc. of the International Conference on Engineering of Reconfigurable Systems & Algorithms, ERSA 2009, Las Vegas, Nevada, USA", July 2009.

International Peer-Reviewed Conference/Proceedings

[33] E. CASSEAU, B. L. GAL. *High-Level Synthesis for the Design of FPGA-based Signal Processing Systems*, in "Proc. of the International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (IC-SAMOS), Samos, Greece", July 2009, p. 25-32.

[34] R. CHOKSHI, A. SHRIVASTAVA, K. S. BEREZOWSKI, S. J. PIESTRAK. *Exploiting residue number system for power-efficient digital signal processing in embedded processors*, in "Proc. of the IEEE/ACM International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES), Grenoble, France", ACM, October 2009, p. 19-28.

[35] S. COLLANGE, D. DEFOUR, A. TISSERAND. *Power Consumption of GPUs from a Software Perspective*, in "Proc. of the 9th International Conference on Computational Science (ICCS), Baton Rouge, Louisiana, U.S.A.", Lecture Notes in Computer Science (LNCS), vol. 5544, Springer-Verlag, May 2009, p. 914–923.

[36] A. COURTAY, J. LAURENT, O. SENTIEYS, N. JULIEN. *Interconnect Explorer: A High-level Power Estimation Tool for On-Chip Interconnects*, in "Proc. of the IEEE/ACM Design Automation Conference (DAC), User Track, San Francisco, USA", 2009.

[37] A. COURTAY, J. LAURENT, O. SENTIEYS, N. JULIEN. *Novel Cross-Transition Elimination Technique Improving Delay and Power Consumption for On-Chip Buses*, in "Proc. of the IEEE International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS), Lisbon, Portugal", Lecture Notes in Computer Science (LNCS), vol. 5349, Springer-Verlag, March 2009, p. 359–368.

[38] A. COURTAY, J. LAURENT, O. SENTIEYS, N. JULIEN. *On-chip interconnects energy consumption: High-level estimation and architectural optimizations*, in "PhD forum of IEEE/ACM Design, Automation & Test in Europe Conference, DATE'09, Nice, France", 2009.

[39] F. DEMANGEL, N. FAU, N. DRABIK, F. CHAROT, C. WOLINSKI. *A generic architecture of CCSDS Low Density Parity Check decoder for near-earth applications*, in "Proc. of the IEEE/ACM Design, Automation & Test in Europe Conference & Exhibition, DATE '09, Nice, France", April 2009, p. 1242-1245.

[40] L. DEVAUX, D. CHILLET, S. PILLEMENT, D. DEMIGNY. *Flexible Communication Support For Dynamically Reconfigurable FPGA*, in "Proc. of the Southern Programmable Logic Conference, Sao-Carlos, Brazil", April 2009, p. 65-70.

[41] L. DEVAUX, S. B. SASSI, S. PILLEMENT, D. CHILLET, D. DEMIGNY. *DRAFT: Flexible Interconnection Network for Dynamically Reconfigurable Architectures*, in "Proc. of the IEEE International Conference on Field-Programmable Technology (FPT'09), Sydney, Australia", IEEE, December 2009.

[42] M. DJENDI, A. GILLOIRE, P. SCALART. *Comparative study of new blind source separation structures for two-channel acoustic noise cancellation*, in "Proc. of the XVII European Signal and Image Processing Conference (EUSIPCO'09), Glascow, Scotland", EURASIP, August 2009.

[43] B. L. GAL, E. CASSEAU. *Automated Multimode System Design for High Performance DSP Applications*, in "Proc. of the European Signal and Image Processing Conference (EUSIPCO), Glascow, Scotland", EURASIP, August 2009.

[44] P. GIORGI, T. IZARD, A. TISSERAND. *Comparison of Modular Arithmetic Algorithms on GPUs*, in "Proc. of the International Conference on Parallel Computing (ParCo), Lyon, France", September 2009.

[45] S. M. A. H. JAFRI, S. J. PIESTRAK, O. SENTIEYS. *Design of a fault-tolerant coarse-grained reconfigurable architecture: A case study*, in "Proc. of the 11th IEEE International Symposium on Quality Electronic Design (ISQED 2010), San Diego, CA, USA", IEEE, March 2010, -, to appear.

[46] S. KHAN, E. CASSEAU, D. MENARD. *Reconfigurable SWP Operator for Multimedia Processing*, in "Proc. of the 20th IEEE International Conference on Application-Specific Systems, Architectures and Processors, Boston, MA, USA", IEEE Computer Society, 2009, p. 199-202.

[47] S. KHAN, E. CASSEAU, D. MENARD. *SWP for multimedia operator design*, in "Proc. of the Conference on Sciences of Electronic, Technologies of Information and Telecommunications, SETIT, Hammamet, Tunisia", March 2009.

[48] J. LALLET, S. PILLEMENT, O. SENTIEYS. *xMAML: a Modeling Language for Dynamically Reconfigurable Architectures*, in "Proc. of the 12th Euromicro Conference on Digital System Design: Architectures, Methods and Tools (DSD), Patras, Greece", August 2009, p. 680 - 687, http://dx.doi.org/10.1109/DSD.2009.151.

[49] L. LEPAULOUX, P. SCALART, C. MARRO. *An efficient low-complexity algorithm for crosstalk-resistant adaptive noise canceller*, in "Proc. of the XVII European Signal and Image Processing Conference (EUSIPCO'09), Glascow, Scotland", EURASIP, August 2009.

[50] K. MARTIN, C. WOLINSKI, K. KUCHCINSKI, A. FLOCH, F. CHAROT. *Constraint-Driven Identification of Application Specific Instructions in the DURASE system*, in "Proc. of Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS), Samos, Greece", Lecture Notes in Computer Science, vol. 5657, Springer, July 2009, p. 194-203.

[51] K. MARTIN, C. WOLINSKI, K. KUCHCINSKI, A. FLOCH, F. CHAROT. *Constraint-Driven Instructions Selection and Application Scheduling in the DURASE system*, in "Proc. of the 20th IEEE International Conference on Application-Specific Systems, Architectures and Processors, Boston, MA, USA", IEEE Computer Society, July 2009, p. 145-152.

[52] D. MENARD, E. CASSEAU, S. KHAN, O. SENTIEYS, S. CHEVOBBE, S. GUYETANT, R. DAVID. *Reconfigurable Operator Based Multimedia Embedded Processor*, in "Proc. of the 5th International Workshop on Reconfigurable Computing: Architectures, Tools and Applications", Lecture Notes in Computer Science, vol. 5453, Springer, 2009, p. 39–49.

[53] Q.-T. NGO, O. BERDER, P. SCALART. *3-D minimum Euclidean distance based sub-optimal precoder for MIMO spatial multiplexing systems*, in "Proc. of IEEE International Conference on Communications (ICC), Cape Town, South Africa", June 2010, to appear.

[54] Q.-T. NGO, O. BERDER, B. VRIGNEAU, O. SENTIEYS. *Minimum Distance Based Precoder for MIMO-OFDM Systems Using a 16-QAM Modulation*, in "Proc. of the IEEE International Conference on Communications (ICC), Dresden, Germany", June 2009, p. 1–5.

[55] T.-D. NGUYEN, O. BERDER, O. SENTIEYS. *Cooperative strategies comparison for infrastructure and vehicle communications in CAPTIV*, in "Proc. of the 9th International Conference on ITS Telecommunication (ITST), Lille, France", October 2009.

[56] H. NGUYEN, D. MENARD, O. SENTIEYS. *Design of Optimized Fixed-point WCDMA Receiver*, in "Proc. of the XVII European Signal and Image Processing Conference (EUSIPCO'09), Glascow, Scotland", EURASIP, August 2009.

[57] H.-N. NGUYEN, D. MENARD, O. SENTIEYS. *Dynamic Precision Scaling for Low Power WCDMA Receiver*, in "Proc. of the IEEE International Symposium on Circuits and Systems, ISCAS 2009, Taipei, Taiwan", May 2009, p. 205-208.

[58] K. PARASHAR, R. ROCHER, D. MENARD, O. SENTIEYS. *A Hierarchical Methodology for Word-Length Optimization of Signal Processing Systems*, in "Proc. of the 23rd International Conference on VLSI Design, Bangalore, India", January 2010, to appear.

[59] M. A. PASHA, S. DERRIEN, O. SENTIEYS. *Toward Ultra Low-Power Hardware Specialization of a Wireless Sensor Network Node*, in "Proc. of the 13th IEEE International Multitopic Conference, INMIC 2009, Islamabad, Pakistan", December 2009.

[60] M. A. PASHA, S. DERRIEN, O. SENTIEYS. *Ultra Low-Power FSM for Control Oriented Applications*, in "Proc. of the IEEE International Symposium on Circuits and Systems, ISCAS 2009, Taipei, Taiwan", May 2009, p. 1577 - 1580.

[61] M. PHAM, S. PILLEMENT, D. DEMIGNY. *A Fault-Tolerant Layer For Dynamically Reconfigurable Multi-Processor System-On-Chip*, in "Proc. of the International Conference on ReConFigurable Computing and FPGAs, ReConFig'09, Cancun, Mexico", December 2009.

[62] M. PHAM, S. PILLEMENT, D. DEMIGNY. *Reconfigurable ECU Communications in Autosar Environment*, in "Proc. of the 9th International Conference on ITS Telecommunications, Lille, France", October 2009.

[63] S. PILLEMENT, D. CHILLET, Y. OLIVA, J. C. PREVOTET. *High-Level Exploration for Dynamic Reconfiguration Management*, in "Proc. of the International Conference on Engineering of Reconfigurable Systems & Algorithms, ERSA 2009, Las Vegas, Nevada, USA", CSREA Press, July 2009.

[64] S. PILLEMENT, D. CHILLET. *High-level Model of Dynamically Reconfigurable Architectures*, in "Proc. of the Conference on Design and Architectures for Signal and Image Processing (DASIP), Nice, France", September 2009.

[65] R. SANTORO, O. SENTIEYS, S. ROY. *On-Line Monitoring of Random Number Generators for Embedded Security*, in "Proc. of the IEEE International Symposium on Circuits and Systems, ISCAS 2009, Taipei, Taiwan", May 2009, p. 3050 - 3053, http://dx.doi.org/10.1109/ISCAS.2009.5118446.

[66] R. SANTORO, O. SENTIEYS, S. ROY. *On-the-Fly Evaluation of FPGA-Based True Random Number Generator*, in "Proc. of the IEEE Computer Society Annual Symposium on VLSI, ISVLSI'09, Tampa, Florida, USA", May 2009, p. 55-60, http://dx.doi.org/10.1109/ISVLSI.2009.33.

[67] R. SANTORO, A. TISSERAND, O. SENTIEYS, S. ROY. *Arithmetic operators for on-the-fly evaluation of TRNGs*, in "Proc. of the Advanced Signal Processing Algorithms, Architectures and Implementations XVIII, San Diego, CA, USA", vol. 7444, SPIE, August 2009, p. 1–12.

[68] A. TISSERAND. *Function Approximation based on Estimated Arithmetic Operators*, in "Proc. of the 43th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, California, U.S.A.", IEEE, October 2009.

[69] C. WOLINSKI, K. KUCHCINSKI, E. RAFFIN, F. CHAROT. *Architecture-Driven Synthesis of Reconfigurable Cells*, in "Proc. of the 12th Euromicro Conference on Digital System Design: Architectures, Methods and Tools (DSD), Patras, Greece", September 2009, p. 531 - 538, http://dx.doi.org/10.1109/DSD.2009.183.

National Peer-Reviewed Conference/Proceedings

[70] L. DEVAUX, S. B. SASSI, S. PILLEMENT, D. CHILLET, D. DEMIGNY. *Réseau d'interconnexion flexible pour architecture reconfigurable dynamiquement et partiellement*, in "Proc. of the Symposium en Architecture de machines (SympA'13), Toulouse, France", September 2009.

[71] H. DUBOIS, O. BERDER, G. GARNIER, B. VRIGNEAU, O. SENTIEYS. *Architecture optimisée de SVD pour le calcul d'un précodeur dans une chaine de transmission MIMO.*, in "Proc. of the 22nd Symposium on Signal and Image Processing (GRETSI), Dijon, France", September 2009, p. 301–304.

[72] A. EICHE, D. CHILLET, S. PILLEMENT, O. SENTIEYS. *Flot d'ordonnancement pour architecture reconfigurable*, in "Proc. of the Symposium en Architecture de machines (SympA'13), Toulouse, France", September 2009.

[73] J. LALLET, S. PILLEMENT, O. SENTIEYS. *Plate-forme de Conception d'Architectures Reconfigurables Dynamiquement pour le Domaine du TSI*, in "Proc. of the 22nd Symposium on Signal and Image Processing (GRETSI)", September 2009, p. 210-215.

[74] K. MARTIN, C. WOLINSKI, K. KUCHCINSKI, A. FLOCH, F. CHAROT. *Sélection automatique d'instructions et ordonnancement d'applications basés sur la programmation par contraintes*, in "Proc. of the Symposium en Architecture de machines (SympA'13), Toulouse, France", September 2009.

Workshops without Proceedings

[75] C. BEAUMIN-PALUD. *Gestion de la mémoire pour la réutilisation de pixels dans les algorithmes d'estimation de mouvement*, in "National Workshop of the GdR SoC-SiP (System-On-Chip & System-In-Package), Paris, France", June 2009.

[76] O. BERDER. *CAPTIV : Consommation et strAtégies cooPératives pour les Transmissions entre infrastructures et Véhicules*, in "Première Conférence Francophone sur les Technologies de l'Information, de la Communication et de la Géolocalisation dans les Systèmes de Transports (CoGIST), Saint-Quay-Portrieux, France", June 2009.

[77] K. MARTIN. *Extraction automatique d'instructions spécialisées en utilisant la programmation par contraintes*, in "National Workshop of the GdR SoC-SiP (System-On-Chip & System-In-Package), Paris, France", June 2009.

[78] K. MARTIN, C. WOLINSKI, K. KUCHCINSKI, A. FLOCH, F. CHAROT. *Design of Processor Accelerators with Constraints*, in "SweConsNet Workshop, Linkoping, Sweden", 2009.

[79] Y. OLIVA-VENEGAS, J.-C. PREVOTET, F. NOUVEL, S. PILLEMENT, D. CHILLET. *Exploration for Dynamic Reconfiguration Management*, in "Sophia Antipolis MicroElectronics Forum, SAME 2009", September 2009.

[80] R. SANTORO. *Evaluation of TRNGs under Various Experimental Conditions*, in "7th International Workshop on Cryptographic Architectures Embedded in Reconfigurable Devices", June 2009.

[81] R. SANTORO. *Évaluation de TRNG dans diverses conditions expérimentales*, in "Crypto'Puces", July 2009.

[82] A. TISSERAND. *Redundant Number Systems for Reconfigurable Arithmetic Units*, in "7th International Workshop on Cryptographic Architectures Embedded in Reconfigurable Devices", June 2009.

References in notes

[83] *AIS 31: Functionality Classes and Evaluation Methodology for Physical Random Number Generators. Version 1 (25.09.2001) (mandatory if a German IT security certificate is applied for; English translation)*, 2001.

[84] A. AHMADINIA, C. BOBDA, M. BEDNARA, J. TEICH. *A new approach for on-line placement on reconfigurable devices*, in "18th International Parallel and Distributed Processing Symposium, 2004.", 2004.

[85] Z. ALLIANCE. *Zigbee specification*, n^{o} ZigBee Document 053474r06, Version, ZigBee Alliance, 2005, Technical report.

[86] V. BAUMGARTE, G. EHLERS, F. MAY, A. NÜCKEL, M. VORBACH, M. WEINHARDT. *PACT XPP — A Self-Reconfigurable Data Processing Architecture*, in "The Journal of Supercomputing", vol. 26, n^{o} 2, 2003, p. 167–184.

[87] C. BOBDA. *Introduction to Reconfigurable Computing: Architectures Algorithms and Applications*, Springer, 2007.

[88] C. BOBDA, M. MAJER, D. KOCH, A. AHMADINIA, J. TEICH. *A Dynamic NoC Approach for Communication in Reconfigurable Devices*, in "Proceedings of International Conference on Field-Programmable Logic and

Applications (FPL), Antwerp, Belgium", Lecture Notes in Computer Science (LNCS), vol. 3203, Springer, August 2004, p. 1032–1036.

[89] D. CHILLET, S. PILLEMENT, O. SENTIEYS. *A Neural Network Model for Real-Time Scheduling on Heterogeneous SoC Architectures*, in "IEEE International Joint Conference on Neural Networks, IJCNN'07, Orlando, FL", August, 12-17 2007.

[90] K. COMPTON, S. HAUCK. *Reconfigurable computing: a survey of systems and software*, in "ACM Comput. Surv.", vol. 34, n^{o} 2, 2002, p. 171–210, http://doi.acm.org/10.1145/508352.508353.

[91] G. CONSTANTINIDES, P. CHEUNG, W. LUK. *Wordlength optimization for linear digital signal processing*, in "IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems", vol. 22, n^{o} 10, October 2003, p. 1432- 1442.

[92] K. DANNE, R. MUHLENBERND, M. PLATZNER. *Executing hardware tasks on dynamically reconfigurable devices under real-time conditions*, in "International Conference on Field Programmable Logic and Applications", Lecture Notes in Computer Science, 2006.

[93] R. DAVID, S. PILLEMENT, O. SENTIEYS. *Energy-Efficient Reconfigurable Processssors*, in "Low Power Electronics Design", C. PIGUET (editor), Computer Engineering, Vol 1, chap. 20, CRC Press, August 2004.

[94] A. DEJONGHE, B. BOUGARD, S. POLLIN, J. CRANINCKX, A. BOURDOUX, L. VAN DER PERRE, F. CATTHOOR. *Green Reconfigurable Radio Systems*, in "Signal Processing Magazine, IEEE", vol. 24, n^{o} 3, 2007, p. 90–101.

[95] A. DUNKELS, B. GRONVALL, T. VOIGT. *Contiki-a lightweight and flexible operating system for tiny networked sensors*, in "Proceedings of the First IEEE Workshop on Embedded Networked Sensors", 2004.

[96] C. EBELING, D. CRONQUIST, P. FRANKLIN. *RaPiD - Reconfigurable Pipelined Datapath*, in "International Workshop on Field Programmable Logic and Applications, Darmstadt", Lecture notes in Computer Science 1142, September 1996, p. 126–135.

[97] A. M. FAHIM. *Clock Generators for SOC Processors: Circuits and Architectures (Text, Speech & Language Technology)*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005.

[98] R. HARTENSTEIN. *A Decade of Reconfigurable Computing: A Visionary retrospective*, in "Design Automation and Test in Europe (DATE 01), Munich, Germany", March 2001.

[99] R. HARTENSTEIN, M. HERZ, T. HOFFMAN, U. NAGELDINGER. *Using The KressArray for Configurable Computing*, in "Configurable Computing: Technology and Applications, Proc. SPIE 3526, Bellingham, WA", November 1998, p. 150–161.

[100] W. KILLMANN, W. SCHINDLER. *A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators*, T-Systems debis Systemhaus Information Security Services and Bundesamt für Sicherheit in der Informationstechnik (BSI), 2001, Technical report.

[101] S. KIM, W. SUNG. *Word-Length Optimization for High Level Synthesis of Digital Signal Processing Systems*, in "IEEE Workshop on Signal Processing Systems, Boston", October 1998, p. 142-151.

[102] K. KUM, J. KANG, W. SUNG. *AUTOSCALER for C: An optimizing floating-point to integer C program converter for fixed-point digital signal processors*, in "IEEE Transactions on Circuits and Systems II - Analog and Digital Signal Processing", vol. 47, n° 9, September 2000, p. 840-848.

[103] P. L'ECUYER, R. SIMARD. *TestU01: A C library for empirical testing of random number generators*, in "ACM Trans. Math. Softw.", vol. 33, n° 4, 2007, 22, http://doi.acm.org/10.1145/1268776.1268777.

[104] M. LEE, H. SIGNH, G. LU, N. BAGHERZADEH, F. KURDAHI. *Design and Implementation of the MorphoSys Reconfigurable Computing Processor*, in "Journal of VLSI and Signal Processing-Systems for Signal, Image and Video Applications", vol. 24, n° 2, March 2000, p. 147–164.

[105] T. MARESCAUX, V. NOLLET, J. MIGNOLET, A. BARTICA, W. MOFFATA, P. AVASAREA, P. COENEA, D. VERKEST, S. VERNALDE, R. LAUWEREINS. *Run-time support for heterogeneous multitasking on reconfigurable SoCs*, in "the VLSI journal", vol. 38, 2004, p. 107–130, http://doi.acm.org/10.1145/996566.996637.

[106] G. MARSAGLIA. *Diehard: A Battery of Tests of Randomness*, Florida State University, Tallahassee, FL, USA, 1996, http://stat.fsu.edu/pub/diehard/, Technical report.

[107] D. MENARD, D. CHILLET, F. CHAROT, O. SENTIEYS. *Automatic Floating-point to Fixed-point Conversion for DSP Code Generation*, in "International Conference on Compilers, Architectures and Synthesis for Embedded Systems 2002 (CASES 2002), Grenoble", October 2002.

[108] D. MENARD, D. CHILLET, O. SENTIEYS. *Floating-to-fixed-point Conversion for Digital Signal Processors*, in "EURASIP Journal on Applied Signal Processing (JASP), Special Issue Design Methods for DSP Systems", vol. 2006, n° 1, 2006.

[109] T. MIYAMORI, K. OLUKOTUN. *REMARC : Reconfigurable Multimedia Array Coprocessor*, in "IEICE Transactions on Information and Systems E82-D", February 1999, p. 389–397.

[110] W. A. NAJJAR, W. BOHM, B. A. DRAPER, J. HAMMES, R. RINKER, J. R. BEVERIDGE, M. CHAWATHE, C. ROSS. *High-Level Language Abstraction for Reconfigurable Computing*, in "Computer", vol. 36, n° 8, 2003, p. 63-69, http://doi.ieeecomputersociety.org/10.1109/MC.2003.1220583.

[111] V. NOLLET, T. MARESCAUX, D. VERKEST, J.-Y. MIGNOLET, S. VERNALDE. *Operating-system controlled network on chip*, in "Proceedings of the 41st annual Conference on Design automation", 2004, p. 256–259, http://doi.acm.org/10.1145/996566.996637.

[112] PHILIPS. *Silicon Hive*, Philips Inc., 2003, http://www.siliconhive.com, Technical report.

[113] B. J. PHILLIPS, D. R. KELLY, B. W. NG. *Estimating adders for a low density parity check decoder*, in "Proc. Advanced Signal Processing Algorithms, Architectures, and Implementations XVI, San Diego, CA, USA", F. LUK (editor), vol. 6313, SPIE, August 2006, 631302, http://dx.doi.org/10.1117/12.680199.

[114] J. RABAEY. *Reconfigurable Processing: The Solution to Low-Power Programmable DSP*, in "IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)", vol. 1, 1997, p. 275–278.

[115] A. RUKHIN, J. SOTO, J. NECHVATAL, M. SMID, D. BANKS. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Statistical Applications*, in "NIST Special Publication in Computer Security", 2001, p. 800-22.

[116] R. SALEH, S. WILTON, S. MIRABBASI, A. HU, M. GREENSTREET, G. LEMIEUX, P. PANDE, C. GRECU, A. IVANOV. *System-on-chip: reuse and integration*, in "Proceedings of the IEEE", vol. 94, n^{o} 6, 2006, p. 1050– 1069.

[117] W. SCHINDLER, W. KILLMANN. *Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications*, in "CHES '02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, London, UK", Springer-Verlag, 2003, p. 431–449.

[118] T. TODMAN, G. CONSTANTINIDES, S. WILTON, O. MENCER, W. LUK, P. CHEUNG. *Reconfigurable computing: architectures and design methods*, in "IEE Proc.-Comput. Digit. Tech.", vol. 152, n^{o} 2, March 2005.

[119] G. VENKATARAMANI, W. NAJJAR, F. KURDAHI, N. BAGHERZADEH, W. BOHM, J. HAMMES. *Automatic compilation to a coarse-grained reconfigurable system-on-chip*, in "Trans. on Embedded Computing Systems", vol. 2, n^{o} 4, 2003, p. 560–589, http://doi.acm.org/10.1145/950162.950167.

[120] E. WAINGOLD, M. TAYLOR, D. SRIKRISHNA, V. SARKAR, W. LEE, V. LEE, J. KIM, M. FRANK, P. FINCH, R. BARUA, J. BABB, S. AMARASINGHE, A. AGARWAL. *Baring it all to software: The raw machine*, in "IEEE Computer", vol. 30, n^{o} 9, September 1997, p. 86–93.

[121] C. WOLINSKI, K. KUCHCINSKI, A. POSTOLA. *UPaK: Abstract Unified Pattern Based Synthesis Kernel for Hardware and Software Systems*, in "University Booth, DATE 2007, Nice, France", May 2007.

[122] Z. A. YE, N. SHENOY, P. BANEIJEE. *A C compiler for a processor with a reconfigurable functional unit*, in "Proceedings of the 2000 ACM/SIGDA eighth international symposium on Field Programmable Gate-Arrays, FPGA '00, New York, NY, USA", ACM Press, 2000, p. 95–100, http://doi.acm.org/10.1145/329166.329187.