

# **ASync 2006**

**13-15 March, Grenoble, France**

## **Circuit Exhibition Booklet**



**Edited by  
Laurent Fesquet  
Gilles Sicard  
Marc Renaudin**



## Table of contents

Asynchronous Microprocessors at Caltech, Caltech	5
FAUST, an Asynchronous Network-on-Chip based Architecture for Telecom Applications, CEA-LETI	6
An Event-driven Processor for Sensor Networks, Cornell University	8
A High-Performance Asynchronous FPGA, Cornell University	9
ASPIDA, Institute of Computer Science, FORTH	10
Fulcrum Microsystems FocalPoint, Fulcrum Microsystems	11
Advanced Processor Technologies, The University of Manchester	12
Time Amplifier Test Chips, University of Newcastle upon Tyne	13
Dual-rail AES Crypto-processor, University of Newcastle upon Tyne	14
High-Speed Fully-Pipelined GCD Chip, Univ. of North Carolina at Chapel Hill	15
Asynchronous ADC, TIMA	16
An asynchronous DES crypto-processor secure against fault attacks, TIMA	18
A Secure Clock-less AES crypto-processor for low-power low-voltage applications, TIMA	20
AMPHIN, An Asynchronous 16*16 Pixel Array-Processor for Morphological Filtering of Greyscale Images, TIMA	22
ASPRO, a 16-bit RISC asynchronous processor, TIMA	24
MICA, an 8-bit asynchronous microcontroller, TIMA	25
TITAC-2: A 32-bit Scalable-Delay-Insensitive Asynchronous Microprocessor, The University of Tokyo	26
Single-Track Full-Buffer (STFB) Chip Results, USC	27
GALS chips of ETH Zurich, ETH Zurich	28



# Asynchronous Microprocessors at Caltech

## Caltech

Caltech, Pasadena CA 91125 USA

Phone: 626 395 6549

Fax: 626 792 4257

E-mail: [alain@async.caltech.edu](mailto:alain@async.caltech.edu)

**Designers:** Steve Burns, Tony Lee, Drazen Borkovic, Pieter Hazewindus, Jose Tierno, Andrew Lines, Rajit Manohar, Mika Nystroem, Uri Cummings, Paul Penzes, Robert Southworth

Foundry: HP CMOS and Vitesse GaAs through MOSIS

Technology: CAM 2micronCMOS, CAM also in 2micron Vitesse HGaAs, FIR Filter 0.9micron CMOS, MiniMIPS 0.6micron CMOS

Month/year of the fabrication: CAM december 1988, Filter 1995, MiniMIPS October 1998

### **Function:**

microprocessors and digital filter

### **Testing results:**

fully functional CAM cmos: 20MIPS, CAM gaas 100MIPS, Filter 500MOPS, MiniMIPS: 180MIPS

### **Detailed specifications:**

Number of transistors or gates: CAM 20K T, MiniMIPS 2M T

Software + library used: Caltech tools and library + MAGIC and SPICE

Design time (man-months): difficult to assess as parts of research projects. total duration of projectsCAM: 6 months, MiniMIPS 3 years.

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): CAM: manual logic synthesis, mixed custom and synthesized layout; MiniMIPS: manual logic synthesis, custom physical design

Test strategy: full functional testing

# **FAUST, an Asynchronous Network-on-Chip based Architecture for Telecom Applications**

## **CEA-LETI**

17, rue des Martyrs, 38054 Grenoble Cedex 9, FRANCE

Phone: 33 4 38 78 25 51

Fax: 33 4 38 78 90 73

E-mail: pascal.vivet@cea.fr

**Designers:** Beigne Edith, Bernard Christian, Clermidy Fabien, Durand Yves, Durupt Jean, Lattard Didier, Varreau Didier, Vivet Pascal

Foundry: STMicroelectronics

Technology: CMOS 130nm HCMOS9GPLL

Category: CMOS digital, research project

Month/year of the fabrication: Sept 2005

### **Function:**

In order to address the design challenges of multi-application SoCs, CEA-LETI has proposed and developed ANOC, an Asynchronous Network-on-Chip architecture. For very large scale integration, the NoC distributed communication architecture is fully scalable and is perfectly adapted to Globally Asynchronous Locally Synchronous (GALS) paradigm, where NOC nodes and links are implemented using Quasi-Delay-Insensitive asynchronous logic while the NoC functional units are implemented with independent clock domains using standard synchronous design methodologies. Dedicated on-chip and off-chip interfaces have been designed to interface the synchronous and asynchronous domains. The proposed ANOC architecture has been successfully applied to the design of a 8 Million equivalent gates prototype chip in 130nm STMicroelectronics technology. The FAUST chip (Flexible Architecture of Unified System for Telecom) integrates a ARM946 core, embedded memories, smart DMA engines, numerous highly programmable HW blocks and reconfigurable data-paths engines. The chip targets 4G Telecom configurable applications and currently implements a Telecom MC-CDMA MIMO application (<http://ist-4more.org>).

### **Testing results:**

The FAUST circuit is currently under test (02/2006). Functional test patterns have been successfully applied to the NoC 2-D mesh architecture while full scan test patterns and memory bists have been applied to the different synchronous NoC units. At full speed in worst case corner, the chip is expected to operate at 150Mhz for the NOC 2-D mesh while the synchronous units are expected to operate at 170 Mhz for a maximum peak power consumption of 1 Watt at 1.2V. A complete prototyping platform has been developed, which integrates 2 FAUST chips and 2 FPGAs connected with the same unified NoC protocol. This application board will be exhibited during the demonstration.

### **Detailed specifications:**

Area (mm<sup>2</sup>): 80 mm<sup>2</sup>

Number of transistors or gates: 8 Million gates (including memories)

Software + library used: STMicro CORELIB's, TIMA TAL library, ARM946 macro

Design time (man-months): 20 MenxYear

Design strategy (VHDL, synthesis,etc.): GALS Noc architecture, VHDL synthesis for synchronous units, TLM/SystemC modelling

**Test strategy:**

functional test patterns for asynchronous 2-D NoC mesh, full scan and bists for all synchronous units

# An Event-driven Processor for Sensor Networks

Cornell University

330 Rhodes Hall, Cornell University, Ithaca, NY 14853

Phone: +1 (607) 255-3553

Fax: +1 (607) 255-9072

E-mail: [rajit@csl.cornell.edu](mailto:rajit@csl.cornell.edu)

**Designers:** Clinton Kelly, IV, Virantha Ekanayake, and Rajit Manohar

Foundry: TSMC

Technology: 180nm

Category: CMOS digital, research project

Month/year of the fabrication: June 2005

## Function:

The chip implements a dual-use asynchronous processor. The first use is as an event-driven asynchronous processor for low power sensor networks. The second use is as a high-performance network simulator for simulating wireless networks.

## Testing results:

We executed many C programs on the processor exercising all the instructions and executing benchmarks that we developed for the wireless sensor network setting. At a duty cycle of 10 events per second (the design requirement), the total power of the processor operating at a 0.66V supply voltage is 0.63 microWatts. At this duty cycle, the power is dominated by leakage in the memories (0.59 microWatts). The peak performance range is 8 MIPS at 0.66V meeting the requirements of the sensor network node, and 129 MIPS at 1.8 V meeting the network simulator requirements.

## Detailed specifications:

Area (mm<sup>2</sup>): 3 sq. mm.

Number of transistors or gates: ~ 500K fets

Software + library used: HSPICE, nanosim. Custom simulation, lvs, analysis tools.

Design time (man-months): 18

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Full-custom with some automated layout

## Test strategy:

Logic analyzer used to examine output probes, processor has I/O interfaces that simplify testing.

# A High-Performance Asynchronous FPGA

Cornell University

330 Rhodes Hall, Cornell University, Ithaca, NY 14853

Phone: +1 (607) 255-3553

Fax: +1 (607) 255-9072

E-mail: [rajit@csl.cornell.edu](mailto:rajit@csl.cornell.edu)

**Designers:** John Teifel and Rajit Manohar

Foundry: TSMC

Technology: 180nm

Category: CMOS digital, research project

Month/year of the fabrication: June 2004

## Function:

The circuit is an asynchronous field-programmable gate array (AFPGA) implemented as an array of pipeline reconfigurable blocks. The architecture of the FPGA uses pipelined interconnects, thereby mitigating the impact of interconnect reconfigurability without complicating the synthesis flow

## Testing results:

At nominal voltage (1.8V) and temperature, the chip operates at a frequency of 674 MHz. The AFPGA operates correctly from 130mV to 2.3V supply voltage at room temperature (294K), with a frequency that ranges from 1.7 KHz to 870 MHz. At 400K, the AFPGA operates correctly from 340mV to 2.3V, with a frequency that ranges from 1.47MHz to 625MHz. In liquid nitrogen (77K), the AFPGA operates correctly from 810mV to 2.3V at a frequency ranging from 31MHz to 1.12GHz.

## Detailed specifications:

Area (mm<sup>2</sup>): 1.75 sq. mm.

Number of transistors or gates: ~ 50K fets

Software + library used: HSPICE. Custom simulation, lvs, analysis tools.

Design time (man-months): 2

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Full-custom

## Test strategy:

Logic analyzer used to examine output probes, re-configurability used to configure on-chip testing.

# ASPIDA

## Institute of Computer Science, FORTH

FORTH-ICS, Vassilika Vouton, Heraklion, Crete, GR 711 10 Greece

Phone: +30 2810 391 667

Fax: +30 2810 391 601

E-mail: sotiriou@ics.forth.gr

**Designers:** Christos P. Sotiriou

Foundry: IHP

Technology: static CMOS 0.25um

Category: CMOS digital, research project

Month/year of the fabrication: 5/2005

### **Detailed specifications:**

Area (mm<sup>2</sup>): 16.51

Number of transistors or gates: 300K transistors

Software + library used: IHP 0.25 um

Design time (man-months): 24

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): De-synchronization

### **Test strategy:**

Full scan concerning the circuit datapath and self-testing concerning the controllers

# Fulcrum Microsystems FocalPoint

## Fulcrum Microsystems

26775 Malibu Hills Road Suite 200, Calabasas, CA 91301

Phone: 818-871-8138

Fax: 818-871-8101

E-mail: [lines@fulcrummicro.com](mailto:lines@fulcrummicro.com)

**Designers:** 45 employees

Foundry: TSMC

Technology: 130nm FSG LVOD

Category: CMOS digital, industrial project

Month/year of the fabrication: tape-out September 2005

**Function:**

24 port 10G Ethernet switch

**Testing results:**

Full speed, full function, some errata

**Detailed specifications:**

Area (mm<sup>2</sup>): 200

Number of transistors or gates: 105M transistors

Software + library used: CAST language, Fulcrum/Artisan library, Rambus SERDES

Design time (man-months):  $\approx$  300

Design strategy: custom QDI async and synthesized synchronous

**Test strategy:**

scan at wafer and package, functional test, validation, qualification

# Advanced Processor Technologies

## The University of Manchester

School of Computer Science, Manchester M13 9PL UK

Phone: +44 161 275 6129

Fax: +44 161 275 6236

E-mail: [steve.furber@manchester.ac.uk](mailto:steve.furber@manchester.ac.uk)

**Designers:** The Advanced Processor Technologies Group

Foundry: ES2 & GPS, VLSI Technology, VLSI Technology, TSMC

Technology: 1.0 & 0.7, 0.5, 0.35, 0.18 micron CMOS

Category: CMOS digital, research project

Month/year of the fabrication: 1994, 1996, 2000, 2002

### Function:

The Amulet series of processors are asynchronous implementations of the ARM 32-bit RISC architecture, with associated support circuits. Amulet1 is a basic processor core; Amulet2e includes a 4kByte cache/RAM and a flexible external memory interface, and is still used, for example in low-power sensor network systems. Amulet3i was developed as part of a commercial prototype and included an ARM9-class processor, an asynchronous multi-master on-chip bus (MARBLE) and a DMA controller synthesized using Balsa. SPA was our first synthesized asynchronous ARM core, built using Balsa, and was the first use of the CHAIN self-timed network-on-chip interconnect technology.

### Testing results:

All chips were functional and ran standard ARM code. The full-custom processors (Amulet1-3) demonstrated that asynchronous processors are competitive in terms of performance and area, and can have superior power-efficiency than the clocked equivalents. They also have greatly superior electromagnetic emission characteristics. SPA showed that asynchronous design can significantly improve the resistance of smart-card ICs to side-channel attacks such as differential power analysis.

### Detailed specifications:

Area (mm <sup>2</sup> ):	22 & 12, 41, 21 (Async. subsystem), 32
Number of transistors or gates:	58KT, 454KT, 800KT, 14MT
Software + library used:	Compass, Compass, Compass, Balsa
Design time (man-months):	~120, ~120, ~300, ~80
Design strategy (ex: VHDL, synthesis, SC, FC, etc.):	full-custom, full-custom, full-custom, Balsa

### Test strategy:

functional test

# **Time Amplifier Test Chips**

## **University of Newcastle upon Tyne**

Merz Court, Newcastle, NE1 7RU, UK  
E-mail: [Keith.Heron@ncl.ac.uk](mailto:Keith.Heron@ncl.ac.uk)

**Designers:** Abas Amir, Heron Keith  
Foundry: MOSIS  
Technology: 0.18 micron  
Category: CMOS analog or mixed, research project  
Month/year of the fabrication: June 2003

**Function:**  
To permit evaluation of Time Amplifier concept.

**Testing results:**  
A test rig was built to permit calibration of on-chip circuitry and the amplification or stretching of short time intervals was plotted for the two time amplifiers on the chip.

**Detailed specifications:**  
Area (mm<sup>2</sup>): 0.2  
Number of transistors or gates: 3020  
Software + library used: Electric  
Design time (man-months): 12  
Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Synthesis

**Test strategy:**  
Measurement of time periods.

# Dual-rail AES Crypto-processor

University of Newcastle upon Tyne

Merz Court, Newcastle, NE1 7RU, UK

E-mail: [J.P.Murphy@ncl.ac.uk](mailto:J.P.Murphy@ncl.ac.uk)

**Designers:** Murphy Julian, Sokolov Danil

Foundry: AMS

Technology: c35b4 (0.35um)

Category: CMOS digital, research project

Month/year of the fabrication: August 2005

## **Function:**

The chip implements the Advanced Encryption Standard algorithm (AES) using synchronous dual-rail and an alternating spacer protocol, and for comparison a less secure synchronous single-rail version. Using dual-rail logic and an alternating spacer protocol balances the logical switching; in turn the power signature used in a differential power analysis attack becomes less data dependent.

## **Testing results:**

The chip was tested by performing a differential power analysis attack on both the dual-rail and single-rail blocks. An FPGA was used to supply test vectors for encryption while an oscilloscope sampled the voltage changes across a 20 Ohm sampling resistor in line with the chip's power supply i.e. the power consumption. The resultant power signatures were then analysed in Matlab for correlations.

## **Detailed specifications:**

Area (mm<sup>2</sup>): 10mm<sup>2</sup>

Number of transistors or gates: +20k

Software + library used: Cadence/Synopsys/Verimap

Design time (man-months): 4 months

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Verilog, Synthesis, Verimap (conversion to dual-rail), layout

## **Test strategy:**

Digital and Analogue simulation

# High-Speed Fully-Pipelined GCD Chip

## Univ. of North Carolina at Chapel Hill

Dept. of Computer Science, CB3175, UNC, Chapel Hill, NC 27599, USA

Phone: +1-919-962-1832

Fax: +1-919-962-1799

E-mail: [montek@cs.unc.edu](mailto:montek@cs.unc.edu)

**Designers:** Gennette Gill, Ankur Agiwal, and Montek Singh

Foundry: IBM

Technology: 8RF (0.13u CMOS, 8 metal layers)

Category: CMOS digital, research project

Month/year of the fabrication: design taped out December 2005; chips expected March/April 2006.

### Function:

Our chip calculates the greatest common divisor of sets of two 8-bit numbers using Euclid's iterative GCD algorithm. One iteration of the algorithm consists of a subtraction and a conditional assignment. We implement this functionality using a set of 12 pipeline stages. The chip design consists of 8 copies of the GCD iteration hardware connected in a ring. The ring can operate on up to 96 data sets at the same time.

An interface stage allows the ring to operate in 3 modes. In *input mode*, new data is allowed to enter but not to exit. In *computation mode*, the interface stage passes data from the last iteration block to the first iteration block, thereby connecting the circuit into a ring. In *output mode*, the connection between the first and last stages is broken, and data can only be read out.

### Testing results:

We have not been able to test an actual implementation of our chip, because it has not yet returned from fabrication. Simulation results suggest that the fabricated chip will operate between 1.5 and 2 giga-data-items per second.

Our entire chip design actually includes two GCD rings. One has conservative timing margins while the other has *weak spots*—places where we have intentionally created timing violations. These intentional errors allow us to demonstrate our delay fault testing strategies.

### Detailed specifications:

Area (mm<sup>2</sup>): 8mm<sup>2</sup> including padframe (pad limited); core size = 1mm<sup>2</sup>

Number of transistors or gates: 70K transistors

Software + library used: Cadence suite + std-cell libraries from Univ. of Washington and Artisan.

Design time (man-months): 5

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Standard-cell, custom design

### Test strategy:

Testable for stuck-at and delay faults; non-intrusive test approach; at-speed testing through test interface.

# Asynchronous ADC

## TIMA

Concurrent Integrated Systems (C.I.S) Group at TIMA laboratory France

46 av. Felix Viallet, 38031 Grenoble Cedex ,France

Contact: Marc Renaudin

Phone: (33) 4 76 57 48 69

Fax: (33) 4 76 47 38 14

E-mail: [marc.renaudin@imag.fr](mailto:marc.renaudin@imag.fr)

**Designers:** E. Allier, J. Goulier, G. Sicard, L. Fesquet, Saeed Mian Qaisar, E. André, R. Rolland, M. Renaudin

Foundry: ST Microelectronics

Technology: 120 nm CMOS project

Category: CMOS analog and mixed, research project

Month/year of the fabrication: July 2005.

### Function:

The AADC (Asynchronous ADC) is an Analog-to-Digital Converter which is based on the non uniform sampling scheme and designed in an asynchronous way. The principle of uniform sampling is presented in Fig. 1a: samples are equi-spaced in time because sampling is ordered by an external clock of a fixed period  $T_{sample}$ . For non uniform sampling (cf. Fig. 1b),  $2^M-1$  quantization levels are regularly disposed along the amplitude range of the signal ( $M$  will be the hardware resolution of the converter). A sample is captured only when the analog input signal  $V_{in}$  crosses one of these levels. This is named: “level crossing sampling scheme”. Contrarily to classical Nyquist sampling, samples are not regularly spaced out in time, because it depends on the signal variations: the sharper the signal, the closer the samples. Thus, together with the value of the sample  $b_i$ , the time  $Dt_i$  elapsed since the previous sample  $b_{i-1}$  must also be recorded, according to the resolution  $T_C$  of a time basis.

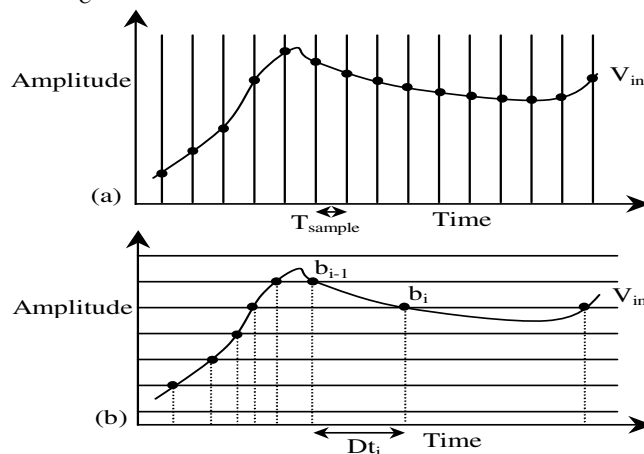


Fig. 1: Regular sampling (a) vs. non uniform sampling (b).

**Testing results:**

The input dynamic of the converter has been set to:  $\Delta V_{in}=600mV$ , centered near  $V_{dd}/2=600mV$ . The maximum frequency, which can be processed by the A-ADC, is  $f_{max} = 160kHz$ . When the chip is running at its maximum speed (worst case), a power consumption of  $180\mu W$  is measured.

**Detailed specifications:**

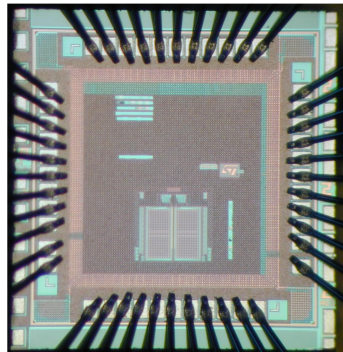
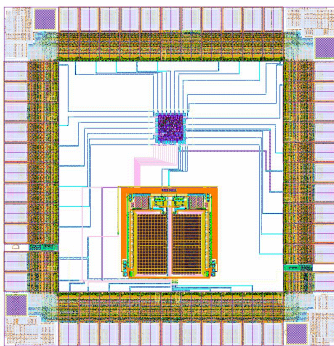
Area (mm<sup>2</sup>): analog area<sub>a</sub> =  $300\mu m \times 320\mu m$ , Digital area =  $95\mu m \times 95\mu m$

Software + library used: HCMOS9 from STMicroelectronics, TAST, Cadence, Soc-Encounter

Design time (man-months): 4 man year

**Test strategy:**

Functional



Figures: AADC layout and chip photography.

# An asynchronous DES crypto-processor secure against fault attacks

## TIMA

Concurrent Integrated Systems (C.I.S) Group at TIMA laboratory France

46 av. Felix Viallet, 38031 Grenoble Cedex ,France

Contact: Marc Renaudin

Phone: (33) 4 76 57 48 69

Fax: (33) 4 76 47 38 14

E-mail: [marc.renaudin@imag.fr](mailto:marc.renaudin@imag.fr)

**Designers:** Yannick Monnet, Fraïdy Bouesse, Marc Renaudin, Sophie Dumont, Nicolas Ninon.

Foundry: STMicroelectronics

Technology: 0.13  $\mu\text{m}$  CMOS (HCMOS9) from STMicroelectronics

Category: CMOS digital, research project

Month/year of the fabrication: October 2004

### Function:

This circuit implements a Clock-Less DES crypto-processor architecture, compliant with the NIST standard: 64 bit data blocks and 64 or 128 bit keys. The circuit implements a standard bus interface enabling an easy connection to any synchronous microprocessors or Asics.

The circuit, powered at 1.2 volt, ciphers a 64 bit data block using a 64 bit key in less than 200 ns which corresponds to a ciphering rate of about 320 Mbits per second. Both a reference version and a fault secured version of the circuit were fabricated.

### Testing results:

Both chips have been designed, fabricated and tested. Their fault resistance level was evaluated using a laser beam fault injection. The countermeasures implemented in the hardened version of the DES were validated.

### Reference DES:

Area (mm<sup>2</sup>): 0.707 mm<sup>2</sup>

Number of transistors or gates: 19.404 kgates

Software + library used: HCMOS9 from STMicroelectronics, TAST, Synopsys, Soc encounter, Cadence

Design time (man-months): 1 man year

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): CHP, VHDL, QDI circuit Synthesis and place and route

### Hardened DES:

Area (mm<sup>2</sup>): 0.707 mm<sup>2</sup>

Number of transistors or gates: 21.409 kgates

Software + library used: HCMOS9 from STMicroelectronics, TAST, Synopsys, Soc encounter, Cadence

Design time (man-months): 1 man year

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): CHP, VHDL, QDI circuit Synthesis and place and route

**Test strategy:**

The functionalities of the circuit were validated with test vectors provided by the NIST (National Institute of Standard and Technology).

From the hardware point of view, the test platform is built of a PC connected to an Altera Excalibur development board. This board includes an FPGA chip which is configured with a 32 bit processor and an interface controlling the asynchronous DES macro cell. An oscilloscope enables measuring the DES chip's speed as well as its power consumption. The oscilloscope is also connected to the PC to automatically capture and store current waves for off-line differential power analysis.

From the software point of view, the ciphering application is running on the PC. It exchanges data with the software running on the 32 bit processor implemented in the FPGA which controls the DES crypto-processor.

# A Secure Clock-less AES crypto-processor for low-power low-voltage applications

## TIMA

Concurrent Integrated Systems (C.I.S) Group at TIMA laboratory France

46 av. Felix Viallet, 38031 Grenoble Cedex ,France

Contact: Marc Renaudin

Phone: (33) 4 76 57 48 69

Fax: (33) 4 76 47 38 14

E-mail: [marc.renaudin@imag.fr](mailto:marc.renaudin@imag.fr)

**Designers:** Fraidy Bouesse, Marc Renaudin, Fabien Germain, Sophie Dumont, Nicolas Ninon.  
Institution: Concurrent Integrated Systems (C.I.S) Group at TIMA laboratory France – SGDN / DCSSI

Foundry: **STMicroelectronics**

Technology: **0.13  $\mu\text{m}$  CMOS (HCMOS9) from STMicroelectronics**

Category: CMOS digital, research project

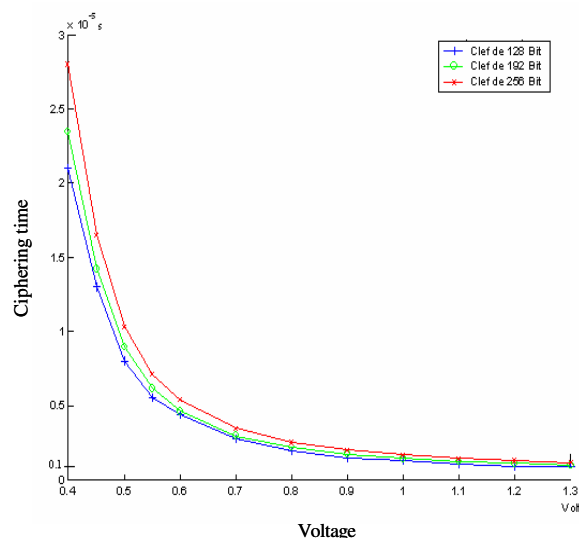
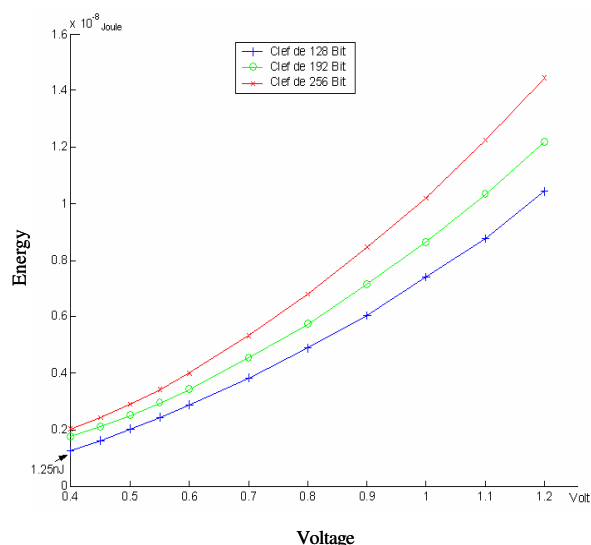
Month/year of the fabrication: **December 2004**

### Function:

This circuit implements a Clock-Less AES crypto-processor architecture, compliant with the NIST standard: 128 bit data blocks and 128, 192 or 256 bit keys. The circuit implements a standard bus interface enabling an easy connection to any synchronous microprocessors or Asics. The circuit, powered at 1.2 volt, ciphers a 128 bit date using a 128 bit key in less than 1  $\mu\text{s}$  which corresponds to a ciphering rate of about 140 Mbits per second.

Due to the robustness of the clock-less Quasi Delay Insensitive logic used to design the chip, the circuit is functional within a wide voltage range, from 1.2 Volt down to 0.4 Volt. This feature is particularly interesting in secure and low-power applications.

### Testing results:



At the nominal voltage (1.2 volt) the circuit consumes about 10 nJ, its throughput is 141 Mbits/s for a key length of 128-bit. The figures above present the variations of energy and ciphering time according to voltage. As illustrated (figures), the circuit powered at 0.4 volt consumes about 1.25 nJ and reaches a throughput of 6.4Mbits/s. The average current is reduced from 11mA at 1.2 Volt down to 200  $\mu$ A at 0.4 Volt.

**Detailed specifications:**

Area (mm<sup>2</sup>): 1.69 mm<sup>2</sup>

Number of transistors or gates: 67.337 Kgates

Software + library used: HCMOS9 from STMicroelectronics, TAST, Synopsys, Soc encounter, Cadence

Design time (man-months): 1 man year

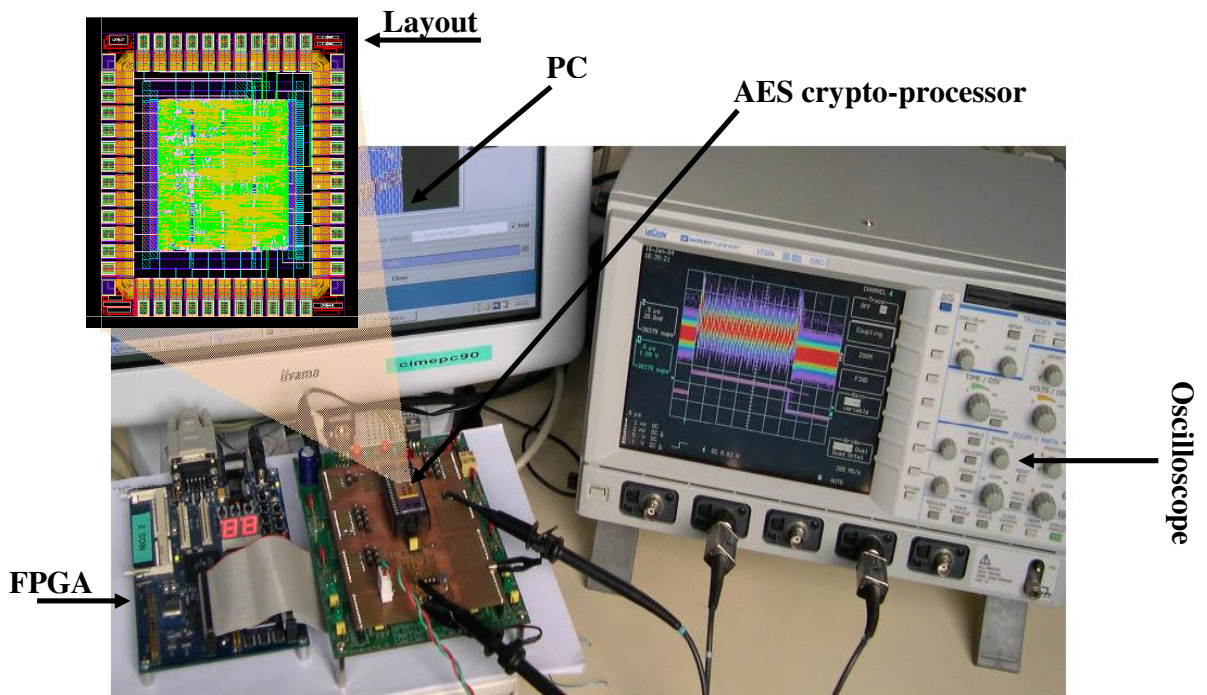
Design strategy (ex: VHDL, synthesis, SC, FC, etc.): CHP, VHDL, QDI circuit Synthesis and place and route

**Test strategy:**

The functionalities of the circuit were validated with test vectors provided by the NIST (National Institute of Standard and Technology).

From the hardware point of view, the test platform is built of a PC connected to an Altera Excalibur development board. This board includes an FPGA chip which is configured with a 32 bit processor and an interface controlling the asynchronous AES macro cell. An oscilloscope enables measuring the AES chip's speed as well as its power consumption. The oscilloscope is also connected to the PC to automatically capture and store current waves for off-line differential power analysis.

From the software point of view, the ciphering application is running on the PC. It exchanges data with the software running on the 32 bit processor implemented in the FPGA which controls the AES crypto-processor.



# AMPHIN, An Asynchronous 16\*16 Pixel Array-Processor for Morphological Filtering of Greyscale Images

## TIMA

Concurrent Integrated Systems (C.I.S) Group at TIMA laboratory France  
46 av. Felix Viallet, 38031 Grenoble Cedex ,France

Contact: Marc Renaudin

Phone: (33) 4 76 57 48 69

Fax: (33) 4 76 47 38 14

E-mail: [marc.renaudin@imag.fr](mailto:marc.renaudin@imag.fr)

**Designers:** Robin Frédéric, Renaudin Marc

Foundry: ST Microelectronics

Technology: 0.5  $\mu\text{m}$

Category: CMOS digital, research project

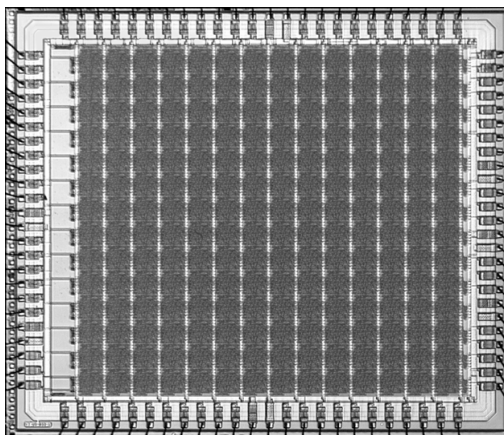
Month/year of the fabrication: 1996

### Function:

We designed a fine-grain asynchronous 16\*16 VLSI array processor. It demonstrates how asynchronism can be exploited both at functional and architectural levels. Our design flow is based on a standard cells approach that combines Differential Cascode Voltage Switch Logic blocks and standard CMOS gates. The chip has been fabricated using the CNET/SGS-Thomson 0.5  $\mu\text{m}$  CMOS triple metal layer technology. It includes 800 000 transistors in an area of 8\*9 mm<sup>2</sup>. It allows real-time iterative morphological filtering of greyscale 256\*256 pixels images at a 30 Hz frame rate using a single chip.

### Testing results:

It has been tested and is fully functional. The peak power consumption is about 1 W at 3.3 V. The maximal execution time of an instruction performing a single iteration step, with the complete neighbourhood and the dual geodesic operation, is 250 ns. It allows real time processing of 256\*256 pixels images at 30 Hz. The chip is still functional at 1.8 V.



Chip microphotograph

**Detailed specifications:**

Area (mm<sup>2</sup>): 72 mm<sup>2</sup>

Number of transistors or gates: 800 000

Software + library used: Standard + Differential Cascode Voltage Switch Logic gates

Design time (man-months): 1.5 man.year

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Specific synthesis procedure. Standard Place and Route tools using specific scripts.

**Test strategy:** functional.

# ASPRO, a 16-bit RISC asynchronous processor

## TIMA

Concurrent Integrated Systems (C.I.S) Group at TIMA laboratory France

46 av. Felix Viallet, 38031 Grenoble Cedex ,France

Contact: Marc Renaudin

Phone: (33) 4 76 57 48 69

Fax: (33) 4 76 47 38 14

E-mail: [marc.renaudin@imag.fr](mailto:marc.renaudin@imag.fr)

**Designers:** Vivet Pascal, Renaudin Marc

Foundry: ST Microelectronics

Technology: 0.25  $\mu\text{m}$

Category: CMOS digital, research project

Month/year of the fabrication: 2000

### **Function:**

We have designed a CMOS standard-cell Quasi-Delay-Insensitive (QDI) 16-bit asynchronous microprocessor using a 0.25  $\mu\text{m}$  technology. ASPRO-216 has been developed for embedded applications. It can be customized both at the hardware and software levels to fit specific application requirements. It is a scalar processor which issues instructions in-order and completes their execution out-of-order. Its architecture extensively uses an overlapping pipelined execution scheme involving de-synchronized units. ASPRO owns four bi-directional serial links with 50 Mb/s throughput, two 16-bit parallel ports, 16 Kwords program memories on chip, and 64 Kbytes data memories on chip.

### **Testing results:**

ASPRO operates with a power supply between 0.65V and 2.5V. The performance of ASPRO-216 is 140 Mips, 0.5 Watt including memories, at 2.5 Volts and 24 Mips, 27 mW, at 1V.

### **Detailed specifications:**

Area (mm<sup>2</sup>): 40 mm<sup>2</sup>

Number of transistors or gates: 6.3 Millions (500 000 for the core)

Software + library used: Standard + Muller gates

Design time (man-months): 3 men.year

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): CHP to VHDL translation and specific synthesis procedure. Standard Place and Route tools using specific scripts.

**Test strategy:** functional

# MICA, an 8-bit asynchronous microcontroller

## TIMA

Concurrent Integrated Systems (C.I.S) Group at TIMA laboratory France

46 av. Felix Viallet, 38031 Grenoble Cedex ,France

Contact: Marc Renaudin

Phone: (33) 4 76 57 48 69

Fax: (33) 4 76 47 38 14

E-mail: [marc.renaudin@imag.fr](mailto:marc.renaudin@imag.fr)

**Designers:** Beigne Edith, Vivet Pascal, Renaudin Marc

Foundry: ST Microelectronics

Technology: 0.25  $\mu\text{m}$

Category: CMOS digital, research project

Month/year of the fabrication: 2000

### Function:

MICA is a QDI asynchronous 8-bit micro-controller CISC machine, based on a dedicated "luxurious" micro-architecture. In order to facilitate the design of a "C" compiler and also to limit memory accesses, we decided to integrate two different register-files: eight 8-bit registers are devoted to data, and eight 16-bit registers are devoted to pointers (including the program counter and the stack pointer). Specific arithmetic units are associated with each register files enabling concurrent computations of data and addresses. A dedicated unit is managing the standard status bits Z, N, V and C. A peripheral unit is also included, supporting six 8-bit parallel ports (1 input, 4 outputs and 1 bi-directional used to control external flash memories and the synchronous/asynchronous interface) and four serial links (using a two-phase delay insensitive protocol compatible with our high performance RISC asynchronous ASPRO processor – described above -). Moreover, the micro-controller integrates 16 Kbytes RAM and 2 Kbytes ROM. The latter includes a *Built-In-Self-Test* which is executed at reset according to the boot mode selected (eight modes are available). It is a 350 assembly instruction routine which performs a complete stuck-at-fault test, thanks to the QDI asynchronous logic. The BIST routine computes a signature written on the fly, on one of the parallel port to report on self-test progress.

### Testing results:

A test chip has been designed, fabricated and tested. The micro-controller has been easily tested thanks to the BIST, and was fully functional at first silicon between 3 Volts down to 0.65 Volt (2.5 Volts is the nominal voltage of the .25 $\mu\text{m}$  CMOS technology used). It is noticeable that the chip only consumes 800  $\mu\text{W}$  at 1 volt, still delivering a computational power of 4.3 MIPS. At 0.8 volt, the chip consumes less than 400  $\mu\text{W}$ .

### Detailed specifications:

Area (mm<sup>2</sup>): 13 mm<sup>2</sup>

Number of transistors or gates: 1 Million (145 000 for the core)

Software + library used: Standard + Muller gates

Design time (man-months): 1 man.year

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): CHP to VHDL translation and specific synthesis procedure. Standard Place and Route tools using specific scripts.

**Test strategy:** functional.

# TITAC-2: A 32-bit Scalable-Delay-Insensitive Asynchronous Microprocessor

**The University of Tokyo**

4-6-1 Komaba, Meguro-ku, Tokyo, Japan

Phone: +81-3-5452-5164

Fax: +81-3-5452-5165

E-mail: [miyabi@hal.rcast.u-tokyo.ac.jp](mailto:miyabi@hal.rcast.u-tokyo.ac.jp)

**Designers:** T. Nanya, A. Takamura, M. Kuwako, M. Imai, T. Fujii, M. Ozawa, I. Fukasaku, Y. Ueno

Foundry: NEC Corporation

Technology: 0.5um, 3Layer Metal, CMOS

Category: CMOS digital, research project

Month/year of the fabrication: Feb. / 1997

## **Function:**

TITAC-2 (Techno-Initiative Tokyo Asynchronous Computer) is a 32-bit asynchronous microprocessor based on the Scalable-Delay-Insensitive model. TITAC-2 is an asynchronous version of MIPS R2000 microprocessor with its 5-stage pipeline structure. TITAC-2 implements an instruction set similar to R2000, including an 8KB instruction cache, 40 32-bit registers, as well as exception handling, external interrupt and memory protection capabilities. The data-path design is based on the 2-rail 4-cycle signaling convention, except for the internal cache and external bus interfaces that use the bundled-data scheme with programmable delay elements incorporated.

## **Testing results:**

The TITAC-2 chip was fabricated by NEC Corporation. It returned from fabrication on Feb.15, 1997. After one-week step-by-step debugging for the processor board, the TITAC-2 chip ran the Dhrystone V2.1 benchmark program successfully on Feb.22, 1997.

The TITAC-2 works correctly with its power supply voltage being varied through the range from 1.5V to 6.0V and the temperature of its package surface being heated up to about 85 degrees Celsius by hair dryer and cooled down with liquid nitrogen, and achieves 54.1 VAX MIPS using the Dhrystone V2.1 benchmark with a power consumption of 2.11W at 3.3V for room temperature.

## **Detailed specifications:**

Area (mm<sup>2</sup>): 12.15mm x 12.15mm

Number of transistors or gates: 496,367 MOS transistors and 8.6K-Byte memory macro

Software + library used: TITAC-2 original library and compiler

Design time (man-months): 100 man-months

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Verilog, Synthesis, Standard cell + Custom asynchronous cell design

# Single-Track Full-Buffer (STFB) Chip Results

## USC

EEB 350, MC 2562, Dept. EE-Systems, USC, USA

Contact: Peter Beerel

Phone: +1-213-740-4481

Fax: +1-213-740-9803

E-mail: [pabeerel@usc.edu](mailto:pabeerel@usc.edu)

**Designers:** Marcos Ferretti, Peter Beerel

Foundry: TSMC

Technology: 0.25 micron

Category: CMOS digital, research project

Month/year of the fabrication: May, 2004

### Function:

This chip demonstrates a high-performance asynchronous template, single-track full-buffer (STFB), which achieves close to full-custom performance using a standard cell design flow and industry standard CAD tools to perform schematic capture, simulation, cell layout, and automatic placement and routing. The chip implements a 64-bit asynchronous prefix adder, and its test circuitry, using the TSMC 0.25  $\mu$ m process. The 64-bit asynchronous prefix adder layout requires 0.96 mm<sup>2</sup> and the entire chip consists of 260k-transistors.

### Testing results:

The chip reaches a measured throughput of 1.45GHz. The design demonstrates that the STFB template can yield three times higher throughput with approximately half of the area of comparable quasi-delay-insensitive (QDI) templates, requires less timing assumptions than ultra-high-speed GasP bundled-data circuits, and can be designed with an automated place & route flow.

### Detailed specifications:

Area (mm<sup>2</sup>): 3.3 mm<sup>2</sup>

Number of transistors or gates: 257k transistors

Software + library used: USC STFB TSMC 0.25 Library (designed using Cadence tools).

Design time (man-months): 6 man-months library development. 6 man-months chip layout

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): Standard-Cell Place and Route

Test strategy: We used an FPGA to load on-chip rings with test vectors and down-sampled results for measurement.

# GALS chips of ETH Zurich

## ETH Zurich

ETZ Zentrum, Gloriastrasse 35, CH-8092 Zurich, Switzerland

Phone: +41 44 632 27 26

Fax: +41 44 632 11 94

E-mail: [kgf@iis.ee.ethz.ch](mailto:kgf@iis.ee.ethz.ch)

**Designers:** Frank K. Gurkaynak, Jens Muttersbach, Stefan Oetiker, Thomas Villiger

Foundry: UMC (Shir-Khan)

Technology: 0.25 (Shir-Khan)

Category: CMOS digital, research project

Month/year of the fabrication: 1/2003 (Shir-Khan)

### Function:

A total of five ASICs have been manufactured during our GALS research:

Fango: GALS demonstrator, Safer Cryptoalgorithm

Marilyn: GALS demonstrator, Safer SK-128 Cryptoalgorithm

Shir-Khan: GALS bus architectures testbed

Oscar: Local clock generator test chip

Acacia: Side-channel attack secure AES implementation

### Detailed specifications:

Area (mm<sup>2</sup>): 25 (Shir-Khan)

Number of transistors or gates: ~3 million transistors (Shir-Khan)

Software + library used: Various

Design time (man-months): ~12

Design strategy (ex: VHDL, synthesis, SC, FC, etc.): VHDL Synthesis

### Test strategy:

Scan based+functional