CDSI team (Circuits, Devices and System Integration)

Themes

MEMS microcomponents:
- microgenerators
- acoustic microsensors
- pressure microsensors

BIOMEMS microsystems:
- asynchronous circuits and systems (asynchronous IP’s, NoCs, GALS, etc…)
- non-uniform sampling and signal processing (algorithms, architectures, circuits)
- reconfigurable asynchronous Logic
- safe and secured robust asynchronous circuits
- smart CMOS vision sensors

Expertise

Scientific
Design, Modeling, Manufacturing and Characterization of MEMS
Modeling, simulation, verification, asynchronous digital and analog circuit synthesis

Fields of expertise
MEMS - Analytic modeling and finite elements
In-IC MEMS
Imagers design, asynchronous design tools, asynchronous systems design

Know-how
MEMS manufacturing in clean-rooms and by rapid prototyping
MEMS optical and electrical characterizations
Development of a logic-cells library, cameras for CMOS imagers, asynchronous circuits prototyping and manufacturing

Industrial transfer
2011: Creation of the UroMEMS company
2007: Creation of the TIEMPO startup company

Research keywords
MEMS, Microsensors, Micro-energy, Micro-acoustics, BioMEMS
Asynchronous circuits and systems, CAD tools, CMOS imagers, non-uniformly sampled digital signal processing

Contact

Skandar BASROUR
UGA Professor
(+33) 4 76 57 43 07
skandar.basrour@univ-grenoble-alpes.fr

Laurent FESQUET
GRENOBLE INP Associate Professor
(+33) 4 76 57 48 12
laurent.fesquet@univ-grenoble-alpes.fr
Energy harvesting has been the subject of intense research over the last decades. Various transduction principles have been presented as potential ways of scavenging the ambient energy (thermal, mechanical, radiative…) and transforming it into usable electrical energy. Among these principles, the piezoelectric transduction is probably the most studied one.

Most of the approaches that we have studied so far were based on resonant piezoelectric devices with working frequencies above 200 Hz. However, our current work is focused on the development of energy harvesters designed to scavenge energy from real vibrational sources. Such a design must take into account a wideband spectral content of an acceleration source centered in a frequency band not exceeding 100 Hz. The dimensional aspects as the geometry and the volume as well as the energy requirements are critical constraints and play important role in the design strategy.

In the following paragraphs, we will describe the simulation, fabrication and characterization of piezoelectric energy harvesters for three different applications.

1. Heart Beat Scavenging

Current version of implantable cardioverter defibrillators (ICDs) and pacemakers consists of a battery-powered pulse generator connected onto the heart through electrical leads inserted through veins. However, it is known that the long-term lead failure may occur and can cause the device dysfunction. When required, the removal of failed leads is a complex procedure associated with a potential risk of mortality. As a consequence, main actors in the field of cardiac rhythm management (CRM) implants prepare miniaturized and autonomous leadless implants, which could be directly placed inside a human heart.

The idea of a stand-alone cardiac implant is not new and several approaches for powering the device have been suggested. More recently, researchers from University of Michigan, Ann Arbor, USA presented simulation results of a piezoelectric energy harvester operating at 40 Hz that could, in theory, power a cardiac implant with heart-induced vibrations. Our industrial and academic partners have measured the heart acceleration signals by placing accelerometers inside several heart cavities of humans and animals. It appears that the heart vibration energy is localized at lower frequencies within a frequency band from 5 to 30 Hz.

We have obtained significant results during the project ‘Heart Beat Scavenging’ (HBS, FUI 2010-13) that aimed at developing the technology of leadless pacemakers. The project gathered experiences from the industry (Sorin, EasiiIC, Cedrat, Tronics) together with the CEA-Léti and the TIMA laboratory. The TIMA laboratory was in charge of the design, fabrication and experimental characterization of a piezoelectric energy harvester prototype operating at very low frequency range (20 to 30 Hz). The device, in its final application, will be excited by the heartbeats and will make part of a new generation of pacemakers. The studied device is beam-like harvester made of two lead zirconate titanate (PZT) thick films assembled in bimorph configuration with dimensions chosen in a way to achieve the resonance in the required frequency range. At the same time, constraints applied on dimensions and generated power must be satisfied.

Heart acceleration signals have been first measured experimentally by placing a 3D accelerometer on heart muscles of both animals and human patients. The spectral content of these signals was studied and the energy distribution of these quasi-periodic signals has been analysed. Given the volume of the leadless pacemaker, we have shown that the PZT layers must be 60 to 65 µm thick in order to comply both with the energy source frequency and the pacemaker energy requirements. However, it appears that none of current fabrication processes can be used for manufacturing of such thick PZT films. Using processes derived from the microelectronic field such as sol-gel deposition or sputtering, the maximum achievable thickness is about 2-5 µm. In contrary, using co-firing techniques, the PZT plates can hardly be thinner than 100 µm. The manufacturing of above described piezoelectric scavenger corresponds to an actual process blind window. As a consequence, we work, in collaboration with the Vermon, s.a., on the implementation of fabrication processes of PZT thick films. We focus on the optimized grinding and polishing techniques of a bulk ceramic material.

After the proof-of-concept of a scaled-up demonstrator of the scavenger operating at 75 Hz, a new device taking into account the geometrical constrains of the real heart ambient has been
fabricated and tested. The prototype (Figure 1) is composed of 2 piezoelectric layers, 60 μm thick, having opposite polarization directions. The layers are attached on a brass shim 12 μm thick. The form of the tungsten seismic mass has been optimized to allow the maximal displacement in the capsule.

Finite elements simulations in ANSYS are used to predict the resonant frequency, the maximal stress level in the beam and the output power with an optimal load resistance under both a harmonic acceleration and a real signal sequence. Figure 2 shows one of the simulation results representing the generated power as a function of the frequency and the resistive load. The characterization of the structure shows a good agreement with the simulation.

Recently, in the framework of the Laureat project in collaboration with Vermon s.a, Livanova and IEF, we have proposed an optimized structure in order to increase the reliability and the lifetime of these devices. These devices present shapes that can reduce the stress concentration located in the clamping part of the device.

2. Micro Thermal Energy Harvester

The aim of this project is to conceive a micro energy harvester able to convert a thermal spatial gradient into usable electrical energy. The transduction is performed in two steps: a first thermo-mechanical conversion transforms the thermal energy into a large mechanical displacement, followed by a second piezoelectric transduction that converts the mechanical displacements into electrical charges. In order to obtain large displacements, the initially curved-down structure is made of two layers with materials having an important mismatch of thermal expansion coefficients. The thermal stresses induced by contacting a hot source are causing a buckling of the clamped-clamped bilayer beam. Once buckled upward, the device is cooled down by convection and buckles down to its initial position, to get again into a contact with the hot source. Measurements carried out on a first macro-prototype have shown promising results.

Micro-prototypes made of aluminium nitride (AlN) and aluminium (Al) have been fabricated using standard CMOS processes in a cleanroom (EPFL) (Figure 3). The devices were electrically characterized at TIMA. A test setup has been built in order to push mechanically the structure from the backside and to initiate the buckling in order to remove the thermal contribution of a final excitation method. An insulating glass tip is mounted on a multilayer stack of piezoelectric material that delivers a defined displacement at a precise frequency to the device. The displacement applied on the structure can then be increased progressively in a way to obtain initially only a linear electrical response and then, after reaching a threshold displacement, a peak response corresponding to the buckling is obtained. As the device is in an unstable position of its buckled state, it is coming back to its original position instantaneously. A power density of 48 nW.cm² is obtained for a 1400 x 700 μm² structure composed of 0.5 μm thick AlN layer and 0.5 μm thick Al layer.

Finally, the prototypes were tested with a thermal actuation. The wafer was placed on a hot plate, whose surface temperature was measured by a thermocouple. By conduction through the silicon wafer, the bilayers were heated up and the butterfly device buckled up at 63 °C. Then, the hot plate was switched off and the device buckled down at 53 °C. The energy furnished by this device during the buckling is estimated at 8 pJ per snap (Figure 4).
The next step is to improve the setup by including a precise measurement of the temperature on the device and not on the hotplate surface, and also by implementing a faster thermal cycling allowing an estimation of the possible power that could be harvested by the structure in the final application.

3. Design and performance optimization of a thermo-magnetically activated piezoelectric generator

The goal of this research is to design a thermo-magnetically activated piezoelectric generator able to convert small ambient temperature variations into electrical energy, which will be usable to power wireless sensors.

Our energy generator can be divided in two main sections based on their functions: the energy transducer and the triggering system. The energy transducer is composed of a piezoelectric bimorph-type cantilever beam. The triggering system consists of two permanent magnets (NdFeB), which are attached to the free end of the beam, and a soft magnetic material (FeNi), fixed under the free end of the beam, forming an air gap. The generator has two operation states: the closed position and the open one. In the initial state (open position), at a cold environmental temperature, the soft magnetic material is magnetized so the cantilever beam is pulled-down due to magnetic force. Later, when the ambient temperature increases, the magnetic properties of the soft magnetic material become paramagnetic, causing the magnetic force to disappear. The beam is pulled back to its initial state because of the spring restoring force. This process of pulling-down and pulling-back of the beam is periodically repeated as long as the energy harvester is placed in an environment with cycled variations of temperature. For visual representation of the energy generator and its performance, the reader is referred to Figure 5.

Based on the approach presented in [4], we developed, using commercial package ANSYS, a coupled multiphysics finite element model (FEM) to analyse the generator behaviour. The validity of this FEM has been verified with experimental results suggesting a reliable estimate. Our proposed FEM promotes a better understanding of the parameters design of such a novel energy generator. Moreover, it offers an effective way to predict and to improve the generator performance. We started by investigating the temperature response of the system; afterwards, the temperature dependent magnetization is studied to finally examining the piezoelectric transduction and the output power.

The maximum average power and average power density of proposed generator are 40µW and 250µW/cm², respectively. Currently, an equivalent model is used for running design optimization algorithms to miniaturize the generator. The next step is to validate optimized design using our FEM and to integrate an energy power management module.

4. References


**Microsystems for Health**

**Keywords:** Medical needle, piezoresistive microgauges, swallowing, physiological signals, MMG

**Members:** A. Bonvilain, B. Kinsiclounon, A. Carriquiry, A. Miailland

**Cooperations:** UroMEMS, IMACTIS, CHU Grenoble, CHU Saint Etienne, TIMC-IMAG, SiMaP

**Contracts:** GAME_D (ANR 2013-2017), LA (Carnot LSI 2015-2018)

1. Piezoresistive microsensors for an instrumented medical needle

Because today a physician has no reliable tool to monitor a medical needle, when he inserted it into the human body, this work deals with an instrumented medical needle, which can be monitored in real time during its insertion. The final goal of this work is to fabricate a prototype to integrate it into a microlocalization tool.

Current localization and navigation tools make the assumption of the non-deformability of the instrument used, often-unchecked assumption in current practice. Indeed, the interactions of the deformable instrument with human tissues (soft tissues, bones, hard obstacles, or others) is causing deformations of the instrument that may result in the failure of interventional medical procedure.

In the practice of surgery, various imaging means are used to detect the deformation of the medical device inserted into the human body.

Imaging methods give clinicians a clear and direct perception of the deformation of the medical instrument in the human body. However, application of these methods is hampered by some existing defects in the accuracy and compatibility.

Faced with these difficulties, it appears necessary to enrich the virtual environments of navigation and representative of reality, giving them the ability to track the exact position of all the deformable instrument and distorted in order to specify, in real time, the relative positions of the instrument, its extremity and the target.

So in our work, we propose to instrument a needle with microgauges. These microsensors allow to measure in real time, during its use, the strain of the needle. We can calculate from this strain the real shape of the needle and give it to the physician, in a previous medical image of the patient.

A microfabrication of microsensors, directly on the body of the needle, has been carried out in a clean room. We have chosen microgauges operating on the principle of the piezoresistivity. This means that during the deformation of the needle, the microgauges on the surface will be deformed, that will cause the change of the value of its resistance [1]. The microgauges are connected to an instrumentation electronic card, which measures the variation of the voltage, allowing the calculation of the variation of the resistance of the microsensor. It allows also the calculation of the deformation and of the deformed shape of the needle. The active material of the microgauges is the germanium.

Classically, the used substrates in clean room are silicon or glass wafer. So we must adapt the process to the unconventional geometry and material of the substrate (needle is circular and in stainless steel).

The needle used for this fabrication are 10 centimeters long and have a diameter of 0.6 millimeters. It is in stainless steel (Fig. 1).

![Figure 1: Microgauge on steel needle](image1)

We have experimented these microsensors after doing a bonding connection. The experimentations consist in making a controlled deflection to the tip of the needle, and to measure the variation of the resistance of the microsensor. The first results show eight straight trajectories (6 mm) of the tip of the needle (2 mm on each side from the non-deformed position, to stay in elastic deformation). Several microgauges are already experimented in the same conditions, and the results are similar. So we can deduce that we have a good repeatability of the measures (Fig. 2).

The different experimentations give an experimental Gauge Factor (GF) of about 20. The commercially microgauges have a GF about 2, so we obtain a better sensitivity.
We have studied the connection of the microgauges. For that, we design needles with their connecting tracks and bonding pads, to export the connections at the proximal extremity of the needle as shown on Fig. 3.

To connect the needle with a microlocalization system, we must design a microconnector, because no solution exist commercially. The most adequate solution is shown on Fig. 4. This solution allow the relatively easy positioning of the needle. Connections are done by 100 µm wire integrated in the parts of the microconnector.

Our works cover the complete study of the instrumented medical needle. It began with the modeling of the needle and the microsensors, and a proof of concept on a macro model. After we have developed the microfabrication process of the microgauges on the needle, and the experimentations was satisfactory, so we have focused on the connections of the microgauges at the proximal extremity of the needle. We have then made needles with microgauges and their connecting tracks, and obtained the expected result. Finally, we have design a microconnector to be able to connect the needle with three microsensors.

We have now to fabricate microgauges on three generatrix of the needle (Fig. 5). For this, we must repeat the same process three times, performing a rotation of the needle of 120° in its support between each process. The microconnector will allow us to connect the micro-gauges with the experimental test bench. We could then monitor the needle in three dimensions. In a longer term, we must integrate the prototype in a microlocalization system to test it.

2. Study of the swallowing and of the associated physiological signals

Our long-term goal is to design an active artificial larynx.

After a state of the art of the domain, we worked on the study of the structure (anatomy and the physiology) and the functions of the larynx. Then, we have studied in the literature the swallowing mechanism, to determine the physiological significant signals in the laryngeal region.

It turns out that the swallowing signal seems reproductive. It is composed of two phases: oral phase and laryngeal phase.

We have so developed a measuring bench of the signals by MMG (MechanoMyoGraphy). It is composed of microsensors (three axes accelerometers), a signal treatment unit with its software (PowerLab with LabChart) and a PC.
The first experimentations consist of the measure of the signal at different position of the microsensor in the laryngeal area. We can so determine the best position of the microsensor for the measurements.

After, to determine the differentiation of the signals, we began to record the phenomena inducing signals such as swallowing, coughing, singing, voice and so on. It seems that the swallowing has a typical signature, which is different of the other phenomena. We tried to characterize the swallowing signal, and to determine the timing of the different phases on a volunteer. Then we studied the swallowing of food of different consistencies. We have shown that the timing is not the same, always on the same person.

The next objective of our work is to record a series of exercises on different people. The exercises can be for example, several swallowing of saliva, water and a more consistent food (brioche or other cake for example). We could then study these signals to determine the repeatability for a same person, and the fidelity of signals from one person to others. This will also allow us to characterize the signals according to the age, the sex and the corpulence of a person. We can see if it is possible to identify the swallowing signal in the middle of other events such as mastication for example (for consistent food).

3. References

1. CMOS-MEMS for acoustics

A successful design of an efficient source generating acoustic pressure in the air by means of vibrating diaphragm must maximize the product of the diaphragm area, its vibrational velocity and frequency. Such a condition limits the exploitation of MEMS-based devices as acoustic sources, in particular in low frequency range, to in-ear or similar applications generating low power signals in closed couplers.

Various approaches to the acoustic generation in air with MEMS use magnetic or piezoelectric materials. Their principal disadvantage is the need to integrate a material that is not a part of a CMOS fabrication process. Another approach consists in digital sound reconstruction involving the summation of discrete acoustic pulses generated by individual acoustic transducers arranged in a matrix and operating in a binary way. Others presented such a digital speaker in a configuration using a capacitive principle.

Recently, works showing the feasibility of MEMS using CMOS technology followed by surface micromachining without mask have been published. Unlike the older approach, where suspended MEMS components were obtained by silicon substrate etching, the proposed technology consists in etching oxide layers resulting from the CMOS process and thus releasing metallic layers of the same CMOS technology. Until now, various applications of this technology were reported and only few of them treat acoustic sources [1].

We show that the industrial 0.35µm CMOS technology can be considered also for sources of airborne acoustic signals. The ultimate goal is the monolithic integration of a device working both as a source and a sensor with electronics, thus facilitating signal routing, suppressing parasitic effects, and improving the signal-to-noise ratio. The acoustic source fabrication is based on AMS 0.35µm CMOS back-end process consisting in the silicon dioxide sacrificial layer removal by hydrofluoric acid (Silox Vapox III) wet etching. The electrostatic transducer structure (Figure 1a) is composed of a squared perforated diaphragm (500 x 500 x 0.925 µm²) and a solid back plate, formed by CMOS metallic layers, separated by an air gap (2.64 µm). The holes size (5 µm) and position on the diaphragm have been chosen to allow a sacrificial layer etching and to avoid an excessive damping due to the air gap. The diaphragm is anchored, through vias.

We have performed the finite element modeling of the acoustic source, followed by the fabrication process and by the device characterization. The preliminary measurement results report the acoustic pressure in the range of tens of mPa generated by the MEMS device at a distance of 10 mm.

2. Haptic Interface

In this project, we work on the design of a new haptic interface that can bring the sense of touch to existing tactile screens. Existing technologies of these interfaces present drawbacks, as the disappointing fineness of the texture, the relatively large electrical consumption (more than 600 mW), the low system integration, or a bulky packaging.

Our project proposes an integrated solution using thin film piezoelectric actuators creating a squeeze film effect on the surface. This device allows a fine texture rendering by changing the friction coefficient.

Our team supports the fabrication of the actuators by the modeling and design. We have built a finite elements model, which takes into account materials of a screen with additional piezoelectric layers. We have also set up a characterization.
bench using a velocimeter to measure the displacement amplitude of the mechanical vibrations. A retrofit of the measured devices has been made, showing a good agreement with the simulation results.

The integration into mobile devices is the most important challenge of this project. To achieve a necessary reduction of the power consumption for the actuation, we have built an equivalent model of the vibration slab based on physical equations. Knowing parameters of the entire system, the vibration frequency can be adjusted in order to provide the highest electro-mechanical transduction.

Thanks to piezoelectric transducers used in a sensor mode, the equivalent model is integrated into the sensor detection in order to reduce the time of frequency adaptation.

A study on those sensors has been made. Figure 2 shows a glass slab with piezoelectric transducers made of thin AlN layer. A characterization of the best position providing the highest feedback signal has been carried-out [3]. A latency time of the entire feedback loop has been established and is compatible with the haptic rendering.

![Figure 2: 110 × 65 mm² glass slab with AlN transducers](image)

These work in process will be exploited by a new start-up company (www.hap2u.net).

3. Polymer-based piezo-electret structures

Piezoelectric polymer materials are of a great interest for their potential integration to sensors and actuators in many applications. Among these applications are wearable devices, electroacoustic transducers, or energy harvesting of mechanical vibrations. Although piezoelectric polymers show lower piezoelectric constants than traditional piezoceramic or crystalline materials, their important advantage resides in a very low Young’s modulus. This property predestines piezoelectric polymers for wearable devices adapted for any shape and size surfaces.

We have concentrated our effort on development of a novel micro-structured material made from PDMS referred as piezo-electret material. In a similar way as other piezoelectric materials, the piezo-electret PDMS can exhibit piezoelectric effect in both actuator and sensor mode due to its anisotropic structure. A micro-structured PDMS layer can be seen as a polymer matrix containing micro-cavities trapping air (Figure 3). The ionization of the air generates opposite charges that are implanted in the inner micro-cavities surfaces, each micro-cavity can be considered as a macro-dipole. The macroscopic dipole moment is determined by the quantity of the charges and the distance separating charges of opposite polarity. So, piezo-electret is sensitive to any external mechanical or electrical stress. In fact, if an external mechanical load is applied on piezo-electret, the distance between opposite charges decreases and compensating charge distribution is generated in conductive electrodes. In the case of externally applied ac-voltage, piezo-electret vibrates periodically. Due to these piezoelectric like effect of piezo-electrets and their low Young’s modulus, they can be utilized as functional materials in electromechanical micro-sensors.

![Figure 3: Schematic illustration of the micro-structured PDMS material with top and bottom gold electrodes](image)

The electromechanical testing carried out on this kind of material shows an output power density of 1 μW.mm⁻³ for a moderate dynamic pressure of 120 Pa at 20Hz.

4. References


CDSI team - 34
Design of Self-timed Circuits

Keywords: Micropipelines, design methods and tools, design for ultra-low power, Petri net models


Cooperations: Starchip IC (SAFRAN), Dolphin, IM2NP, Morpho (SAFRAN), S.P.S., Asulab (SWATCH)

Contracts: LISA (FUI), Expertise contract with SWATCH

1. Context and objectives

This work is done in the frame of LISA (FUI project) and an expertise contract with SWATCH. Its goal is to develop new methods for designing low-power circuits using asynchronous design techniques.

LISA (Ultra-Low power Integrated circuit for Secure RF Applications) addresses the market of contactless smart cards. Their form factor, power consumption and performances are important issues that need to be considered to allow their deployment on a massive scale. The goal of LISA is to reduce by an order of magnitude the power consumption of contactless smart cards: 1) by increasing the amount of energy recovered by the antenna, and 2) by reducing the integrated circuit (IC) power consumption.

Reducing the IC power consumption is obtained by two means. Firstly, the IC is designed with ultra-low power libraries provided by Dolphin. Secondly, new low power architectures are explored for each intellectual property (IP) in the device. The role of TIMA in this project is to develop methods and tools for designing these IPs using asynchronous techniques.

These works are also used in the frame of an expertise contract with Asulab (SWATCH) for designing an ultra-low power processor.

2. A practical framework for the specification and design of self-timed circuits

This work addresses the design of asynchronous micropipelines whose structure is depicted in Figure 1. In the following, we refer to them as self-timed circuits. Their datapaths have the same structure than datapaths in synchronous circuits. However, they do not use a global synchronization signal (clock). The communications between registers are rather assured by distributed controllers which perform local synchronizations.

Self-timed circuits are interesting alternatives to implement low power circuits but they are harder to design. The main goal of this work is to provide a practical environment for designing self-timed circuits, by developing methods for specifying the controller, verifying it, and implementing it.

In this work, formal verification of the control circuit functionality is based on high-level Petri net models. These newly proposed models have a compact representation for memoryless channels by only modeling the token boundaries. Contrarily to the state-of-the-art models, they also take into account choice structures in the controller (splits and merges). They are more compact than traditional models such as signal transition graphs (STG), and thus allow verifying large and complex circuits without combinatory explosion.

To derive these models, we outlined general simplification mechanisms for Petri nets used to model asynchronous controllers. Their formal proof of correctness is based on the concept of bisimilarity. Depending on the required level of granularity, different models can be extracted. A so-called channel-accurate model is obtained by accurately modeling the request paths and minimally modeling the acknowledgement paths. This model can be timed and serves for performance analysis (latency and cycle times). An initialization-independent model is obtained by applying all the simplification which are possible for all the circuit initialization. This model is practical for verification and refinement because it is compact, and it allows the designer to evaluate different circuit initializations.

Along with these models, we describe a practical framework addressing all the design steps of self-timed circuits, from the circuit specification to its physical implementation, using standard EDA tools. We show how TCL scripts can be used to: define relative constraints in the static timing analysis tools (for synthesis, placement and routing), to cut appropriate timing arcs in the control circuit, and to automatically insert delays that match critical paths in the datapath.

3. Results: low-power AES cipher

We applied these methods to design a 128-bit AES (Advanced Encryption Standard) cipher in a 55 nm UMC technology.
The datapath is specified at register transfer level (RTL). A controller is derived from this datapath by a method of templates, i.e. by associating each circuit fragment to an appropriate control sub-circuit. Those sub-circuit are assembled to obtain the controller. This controller is then verified for liveliness using an initialization-independent model, and the appropriate refinements are performed in the control circuit.

Figure 2-a shows the datapath of the AES cipher. In this design, ADD combines the “Add key” operation and key scheduling. SUBSH combines the “Substitute bytes” and “Shift rows” operations. MIX does the “Mix columns” operation. Each module consists of an input combinational block and a bank of 256 registers except ADD which also has an output combinational block. The FSM controls the selection between the first nine rounds and the last round, it contains a 4-bit state register.

![Datapath](image1)

![Control model](image2)

Figure 2:
(a) Datapath of a 128-bit AES cipher.
(b) Associated initialization-independent model

An initialization-independent model is used to verify the circuit for liveliness. Figure 2-b shows the Petri net model for the associated controller after refinement. Dashed arcs represent acknowledgment paths. Arcs weights are used to model conditional branching in the control circuit. Those weights are associated with data sequences $S_m$ and $S_r$, representing data flows of the selection signals.

<table>
<thead>
<tr>
<th>Design</th>
<th>Power consumption (mW)</th>
<th>Area (µm²)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync. AES</td>
<td>9.90</td>
<td>43481</td>
</tr>
<tr>
<td>Gated sync. AES</td>
<td>4.17</td>
<td>45655</td>
</tr>
<tr>
<td>Async. AES</td>
<td>3.76</td>
<td>44273</td>
</tr>
</tbody>
</table>

Table 1: Comparison of three AES implementations with equivalent performances at a nominal voltage of 1.2 V in UMC 55 nm

Table 1 shows a 62% power consumption reduction in the asynchronous design with an area overhead of only 2%. When applying fine grain clock gating to the synchronous design (at each stage), the power consumption is reduced by 58% but with an area overhead of 5%.

4. Conclusion

This work provides practical methods for specifying, verifying, optimizing and physically implementing self-timed circuits. Specification is performed at RTL level while verification is based on a high-level Petri net model. We have demonstrated the method on an AES cipher and a FIR filter. Results for the AES show that the self-timed circuit provided a natural approach for tracking data activity, with lower area overhead and better power consumption reduction than the clock gated circuit.

5. References


Asynchronous Circuits for FDSOI technology

**Keywords:** QDI, design methods and tools, design for ultra-low power, FDSOI technology

**Members:** L. Fesquet, R. Iga, R. Possamai-Bastos, T. Leite, O. Rolloff, J. Simatic, S. Engels, A. Cherkaoui

**Cooperations:** STMicroelectronics, Tiempo, CEA

**Contracts:** Things2Do (ENIAC)

1. **Context and objectives**

Low-voltage operation is an efficient and well-known strategy to save power. Its drawback is the decrease of the circuit speed. The Fully Depleted Silicon on Insulator (FDSOI) technology allows mitigating this speed loss thanks to body biasing. In addition, Quasi Delay Insensitive (QDI) asynchronous circuits use communication protocols which indicate circuit activity. The activity detection is used to activate/deactivate the local block body biasing in order to save energy when blocks are unused. This study tends to define an ideal granularity for biasing delay-insensitive asynchronous circuits in 28-nm FDSOI technology when operating in low-voltage mode.

2. **State of the art**

The innovation brought in this work lies in combining FDSOI features in terms of power management and asynchronous logic for detecting circuit activity. This is particularly promising because asynchronous circuits use handshaking protocols which include explicit signals that can be exploited for triggering and driving voltage and body bias controllers. A first work in this field has been reported in 2013 by CEA-LETI [1].

The main innovation carried out by TIMA and TIEMPO is to design efficient mechanisms able to bias asynchronous blocks with different voltages as fast as the data flow within the architecture. Activity detectors and boost cells, as part of the mentioned mechanisms, provide with latency a steady biasing voltage for asynchronous blocks. Hence, such mechanisms should deliver the body bias voltage with the lowest latency in order to better benefit from the FD-SOI technology when data are processed in the asynchronous blocks. In this context, delay insensitivity of QDI asynchronous circuits is a key feature to exploit, in order to avoid high timing margins that are time-consuming and difficult to characterize.

**Asynchronous Circuits**

Synchronous circuits use a clock signal to synchronize and propagate data. Nowadays, 99% of integrated circuits use a synchronous strategy [4]. It has some advantages as commercial tools and trained experts. However, the use of a clock signal has also its drawbacks. First and foremost, the clock signal demands a significant amount of energy to be produced and distributed. Indeed, the synchronous clock tree generates noise and is able to interfere and disturb other circuit blocks such as analog parts.

Instead of synchronizing with a clock signal, asynchronous circuits use handshake signals to manage data transmission [8][9][10]. In this case, the data flow is locally managed and, thanks to this intrinsic property, the circuit activity is easily detectable. Figure 1 shows a comparison between the synchronous circuit model (a) and its asynchronous counterpart (b).

As it exists several classes of asynchronous circuits, there is a large number of possible implementations. The Quasi Delay Insensitive logic (QDI) is targeted here [4]. These QDI circuits accept a wide range of delays in their wires and gates and allow designing robust circuits using advanced technology nodes.

![Figure 1: Abstraction of (a) Synchronous and (b) Asynchronous logic blocks](image-url)
Intrinsic Features of FDSOI technology

Body biasing in FDSOI technology is one of the most exciting features of this new technology [2][5][7][11]. FDSOI differs from traditional bulk technologies by using a SOI wafer with thin monocrystalline Si layer on the top. First, it isolates the Source and Drain pins from the substrate. This isolation creates a leakage barrier between source-and-substrate and drain-and-substrate as well as it offers new design options.

3. Fine grain body bias with QDI circuits

Low-voltage operation with biasing in FDSOI

Low-voltage is an interesting way to reduce power consumption. Indeed, it is not a new idea and “Vitale et al.” showed the ability on an entire microprocessor in FDSOI technology operating at 0.33 V [12]. Power consumption can be reduced by almost 3 orders of magnitude for a Muller Gate operating at its lowest operating voltage [4]. However, circuits become considerably slower at low-voltage. In this case, the body biasing can be applied to compensate the speed reduction or to alternatively save even more power. To allow the use of biasing, FDSOI technology typically includes a biasing source generator (BBgen) and a biasing tree with a special cell (BBmux), which activates different bias for different area. Nevertheless, this approach only targets a coarse granularity for the body biased area (Typically a processing unit such as processors, cryptoprocessors, etc.).

Autonomous speed and power-control at low-voltage

A self-timed power-control has been to efficiently use the biasing resources. This technique allows to compensate the lost in circuit speed due to the low-voltage operation. However, it is required to implement a complementary control-circuit that activates the biasing source depending on the circuit demand. Moreover, small IPs require smaller biasing energy resource than the BBGEN and the BBMUX tree. As circuit activity can easily be detected thanks to QDI asynchronous handshaking signals, the body bias control can easily be take advantage of these signals. In addition, delay insensitivity allows using different body bias voltages. Our research works have investigated the optimal circuit granularity and also solved backend issues such as the required isolation between each block.

Body bias control

As already mentioned, FDSOI library provides solutions for controlling biasing voltages (BBMUX and BBGEN). However, it has been designed to supply large circuit areas. In this work, new IP blocks have been designed to bias small circuits in order to efficiently bias each block (only when needed), when the data are entering the blocks. For this purpose, activity detection and level shifter circuits detect when new data are entering the block and supplies biasing when needed. Two basic level shifter architectures were studied: the Conventional Level Shifter (CLS) and the Contention Mitigated Level Shifter proposed by Tran et al. [13].

4. A specific FDSOI design flow for asynchronous circuits

TIMA team is developing models and methods for the design of asynchronous systems on FD-SOI. This work aims to save power by associating biasing advantages of FDSOI with intrinsic properties of quasi-delay insensitive (QDI) asynchronous circuits.

Two design flow approaches were specified targeting low-power devices for final applications such as the Internet of Things (IoT). Asynchronous circuits with minimal leakage consumption will be designed with Regular Threshold Voltage (RVT) transistors, Reverse Body Biasing (RBB) schemes, and low operation voltage. The other approach seeks asynchronous circuits with minimal dynamic power consumption by using Low Threshold Voltage (LVT) transistors, Forward Body Biasing (FBB) schemes, and low operation voltage.

The FD-SOI 28-nm standard-cell design flow was developed with Synopsys, Cadence, Mentor and Tiempo (ACC) tools.
5. Conclusion
The simulation results show a real interest in the technique and a testchip has been taped-out and fabricated.

6. References
Cryptographic Key Generation in Hardware

Keywords: TRNG, self-timed rings, stochastic models

Members: A. Cherkaoui, L. Fesquet, G. Gimenez, R. Possamai-Bastos

Cooperations: LaHC, Electronic Marin (SWATCH), Dolphin, Starchip

Contracts: Expertise contract with SWATCH, LISA Project (FUI)

1. Context and introduction

This work has been initiated in the context of a “Région Rhône-Alpes” PhD [1] in collaboration with LaHC (UMR CNRS 5159). Its goal was to explore new TRNG architectures using asynchronous design methods. It has been pursued in 2016 in the frame of an expertise contract with Electronic Marin (SWATCH) and with the support of the LISA project.

True Random Numbers Generators (TRNG) rely on physical random processes to generate random bit sequences. TRNGs used for cryptographic applications with high security requirements (such as key generation for symmetric encryption) not only need to be unpredictable, but they must also be not manipulable. Unpredictability is assessed using a stochastic model whereas the robustness to manipulation and active attacks can be guaranteed by monitoring the entropy source and the entropy extractor in order to detect abnormal behaviors of the generator. Online tests can be applied at startup or on demand to detect statistical defects in the output sequences.

2. Self-timed ring based True Random Numbers Generator (STRNG)

The STRNG leverages the jitter of events propagating in a Self-Timed Ring (STR) to generate provably random numbers at a high throughput. Its architecture and its principle have been proposed in [2]. [3] develops a stochastic model which allows to compute a lower bound of entropy per output bit as a function of design parameters (number of ring stages) and technological parameters (mean propagation delay per stage, jitter per stage). Figure 1 shows that this lower bound increases when we increase the number of STR stages in a given implementation. In [4], we showed how the design can be monitored to detect attacks and abnormal behaviors of the entropy source.

This architecture has been validated in Altera (Cyclone III, IV and V) and Xilinx (Virtex 5, Spartan 6) FPGAs. Figure 2 shows the experimental bench we used for jitter characterization. Three circuits have been designed (two AMS 350 nm circuits and one ST 28 nm circuit). The statistical quality of the output was evaluated using FIPS 140-1, NIST SP800-22 and AIS31 statistical test suites. All those tests pass with throughput as high as 400 Mbit/s in the FPGA designs and 100 Mbit/s in the AMS 350 nm designs.

Presently, CDSI and Electronic Marin study new implementations of this TRNG using under-threshold transistors. Our goal is to reduce the power consumption to the extent that the TRNG can be embedded in an ultra-low energy budget watch. At this point, we have embedded STRs in a first circuit (CMOS 180 nm) for measuring technological parameters in order to size the TRNG. A 180 nm CMOS (from EM) circuit embedding an ultra-low power STRNG has been tape-out and fabricated. The STRNG results demonstrate an outstanding energy efficacy (30pJ/bit at 0.5 Kbit/s) whereas the circuit has a low complexity (305 gates) [5].

CDSI and Dolphin also designed a set of STRNG that have been tape-out in a CMOS 55 nm technology from UMC. Moreover, they developed threat models and the appropriate countermeasures for STRNG [6].

![Figure 1: Lower bound of entropy per output bit (Hm) as a function of the number of STR stages (L) for different ratios jitter standard deviation (sigma) on STR oscillation period (T)](image)

Presently, CDSI and Electronic Marin study new implementations of this TRNG using under-threshold transistors. Our goal is to reduce the power consumption to the extent that the TRNG can be embedded in an ultra-low energy budget watch. At this point, we have embedded STRs in a first circuit (CMOS 180 nm) for measuring technological parameters in order to size the TRNG. A 180 nm CMOS (from EM) circuit embedding an ultra-low power STRNG has been tape-out and fabricated. The STRNG results demonstrate an outstanding energy efficacy (30pJ/bit at 0.5 Kbit/s) whereas the circuit has a low complexity (305 gates) [5].

CDSI and Dolphin also designed a set of STRNG that have been tape-out in a CMOS 55 nm technology from UMC. Moreover, they developed threat models and the appropriate countermeasures for STRNG [6].
3. Conclusion

The main contributions of this work are a new TRNG architecture and its stochastic model. The most important feature of this architecture is its scalability: it can extract provably random numbers (i.e. with an assessment of entropy) no matter the jitter amplitude in a given technology. The associated stochastic model allows the designer to measure technological parameters and, using it, determine the number of required ring stages to achieve the desired security level. Ongoing works are now concentrating on reducing the design’s power consumption by using a library of cells with under- and near-threshold transistors.

4. References


1. Synopsis

The development of modern computers is principally devoted to increasing performance and decreasing size and energy consumption, without any modification of the principles of computation. In particular, all the components must always perform deterministic and exact operations on sets of binary signals. These constraints impede further progress in terms of speed, miniaturization and power consumption. MicroBayes is investigating a radically different approach by using stochastic bit streams to perform calculation. Our goal is to show that stochastic architectures can outperform standard computer when solving complex inference problems such as source localization [6] and separation both in terms of execution speed and power consumption.

The use of non-standard architectures for processing uncertain information is experiencing remarkable growth: see for example the Probabilistic Computing Project at MIT and the Darpa projects PPAML or UPSIDE. One European counterpart is the European project Bambi (Bottom-up Approaches to Machines dedicated to Bayesian Inference. The Bambi project revealed the enormous potential of stochastic computing when considered at the bit level. This potential is even reinforced by the progress made to massively generate random bits with dedicated hardware opening the way, at a very short term, to the design of stochastic computers. We will target three scientific and technical challenges: (a) The study of new algorithm for stochastic inference based on generating sets, (b) the design of non Von Neumann architectures dedicated to process stochastic bit streams [1] and (c) the evaluation of stochastic machines on difficult Bayesian inference problems related to sensor fusion and interpretation.

This radical change to current computation models at the very deepest level of design may very well lead to low-power reactive systems connected to the environment through noisy sensors.

2. A practical framework for demonstrating a stochastic processor

Technically our goal is to demonstrate a working stochastic processor performing localization and source separation from noisy acoustic signals. A success will open new perspectives in sensor processing which will lead to the use of inexpensive and noisy sensors on equipment working with extremely low energy sources. Several compilers will be developed to target several stochastic processors and transform Bayesian programs into dedicated bit wise Gibbs sampler.

New designs will also be devised to build these machines that extensively exploit True Random Number Generators [2][3][4]. From a theoretical stand point, we will characterize the search strategies in high dimension space by studying several generating sets of $[0,1]^n$. In other words, we would like to identify the heuristics used to explore large search space and knowingly apply them to NP problems in a more abstract and possibly more efficient way.

3. Transfer to the Industry

A group of CNRS colleagues are now pushing an industrial transfer of this probabilistic approach. The Zaphod project aims at developing a rebooting computing group inside the company Probayes in order to develop hardware probabilistic computers. The project started during the last trimester of 2017 and planned to hire hardware designers from our team in January 2018. Moreover, a common laboratory between CNRS and Probayes is expected in 2018.
4. Conclusion

We are currently working on an industrial setup to exploit stochastic. Indeed, getting low-power signal processors dealing with noisy sensors is of major interest for the industry, the defense and aerospace industries since recent tests made on the BM1 by TIMA (RIS team) demonstrates the robustness of probabilistic processor to bit flips due to electromagnetic radiations. By providing new results and by developing the knowhow in this emerging field MicroBayes could greatly contribute to push forward this new scientific and industrial endeavor.

5. References

Asynchronous Low-Power Synthesis (ALPS): Tools for Non-Functional Specifications

Keywords: Design methods and tools, design for ultra-low power, non-uniform sampling, Analog-to-Digital Conversion, Petri net models, QDI, micropipelines, electromagnetic compatibility, industrial test


Cooperations: STMicroelectronics, Asulab (Swatch Group), EM (Swatch Group), Gipsa, LJK, VDS, SLS

Contracts: MESR, ANRT, Swatch Group, e-BaCCuSS (Persyval)

1. Context and objectives

This work targets very ambitious objectives because we expect developing several design tools in a unique framework called ALPS. ALPS stands for Asynchronous Low-Power Synthesis but integrates different tools able to provide a wide range of asynchronous solutions to designers.

On one hand, designers face today problems in implementing circuits while the specifications cover not only the design functionalities but also requirements such as power, security, EMC or safety. On the other hand, the asynchronous strategy based on synchronizing circuits thanks to local handshakes offers a wide range of solutions for targeting at design time the non-functional circuit requirements. All these solutions share the asynchronous and event-based approach but also models and theory. Therefore a complete framework has been setup in order to integrate several tools that could be connected together. Notice that these tools are complementary to those included in the commercial design flows.

2. Smart non-uniform sampling schemes

Reducing the power consumption in integrated systems has been the starting point. Indeed, the theoretical and practical researches, pushed in our team since 2000, has highlighted that the Nyquist-Shannon theory tends to capture useless samples [FES 16]. Therefore Level-crossing sampling schemes (LCSS) have been devised and an Asynchronous Analog-to-Digital Converter (A-ADC) has been designed, fabricated and tested.

Based on this sampling scheme, a mathematical theory is under development with the LJK Laboratory (specialized in applied mathematics). Our sampling techniques produce fewer samples than with the traditional Nyquist-Shannon techniques but the samples are not anymore captured thanks to a sampling clock! The consequence of these non-uniform sampling schemes is the non-regular arrival of the data. Nevertheless, this is absolutely not an issue if considering event-driven (asynchronous) circuits. Indeed, thanks to this parsimonious sampling, fewer data are produced. The data arrival produces an event that activates our asynchronous circuits. The rest of the time, the asynchronous circuits remain idle, waiting for the next data (or event).

3. Definition of the ALPS framework

The ALPS framework targets the automated synthesis of integrated systems based on an LCSS analog-to-digital conversion and an event-driven circuit able to process the data captured by the A-ADC [SIM 16-2][SIM 16-3]. The framework offers the opportunity to evaluate the sampling scheme and the appropriate processing [BEY 16][SIM 17][SIM 16-1] thanks to the SPASS library written in Matlab (and partially ported in Python). Once the sampling scheme and the associate signal processing are fixed, the tools ALPS-HLS and ALPS-ADCGen respectively generate a netlist of the processing unit and another one for the A-ADC.
As the designs are specified at an algorithmic level, an automated High-Level Synthesis (HLS) has been targeted. This is done with AUGH, an open software tool developed by the SLS group of the TIMA Laboratory, which has been adapted to our specific design flow.

In order to validate our framework, a FIR filter processing an ECG signal has been implemented and compared to its synchronous counterpart. The results obtained with ALPS show a circuit 12% smaller and an energy consumption reduced by 28% compared to the synchronous FIR filter.

4. Shaping the EM by design

Electromagnetic Compatibility (EMC) specifications have always been a hard task for integrated circuit designers. Indeed, the unwanted generation, propagation and reception of electromagnetic energy in integrated circuits may cause unwanted effects such as electromagnetic interference (EMI) or, even worst, physical damage. Therefore EMC defines the rules and specifications that ensure correct operations of electronic equipment. This work only targets the mitigation of the EM field emitted by a circuit aggressor and tends to respond for the first time to this issue by a design strategy, which could easily be automated. With such an approach, fitting within a spectral mask should become a specific step in the integrated circuit design flow. This task can be ensured by a specific tool ALPS-EMShaper. In order to apply such a strategy, event-based asynchronous circuits have to be targeted. For this purpose micropipeline circuits have been chosen because they offer the required event-driven behavior and an easy implementation. Notice that this design strategy can be extended to any kind of asynchronous circuits. Once the event-driven circuit is designed, the designer has to determine the switching instants of the logic thanks to specific delays accordingly chosen with the specified spectral mask [GER17]. This is done thanks to a genetic algorithm, which computes the delays. We obtain a significant reduction of the electromagnetic spectral peaks with this strategy in comparison to the synchronous spectrum of an equivalent clocked circuit. To enhance the spectrum quality and ease the result convergence, the architecture can be modified to add delays. The range and the step of the delays are two important parameters that can be tuned to more easily fit the spectral mask. In order to validate the approach, a test chip in 40 nm from ST Microelectronics has been designed. It embeds programmable delays in order to validate different hypothesis made when constructing the method.

An example is given Figure 3. The blue curve represents the mask used in the genetic algorithm to evaluate individuals. The red curve is the results of the Matlab GA for a micropipeline of a hundred of delays, the spectrum fits with the mask. The green curve represents the frequency spectrum for the synchronous version of the design with a 10 ns periodic clock.
5. Arithmetical generator for low-power

This work addresses the design of specific asynchronous arithmetical units that can be used for adapting their resolution on events. The goal is here to minimize the circuit activity and thus the power consumption [SKA 17]. This should be also integrated in ALPS.

6. Testing asynchronous logic

In order to fit the industrial needs, a specific strategy for testing event-driven circuits is under investigation. This started end of 2017 and will also be added to our ALPS framework.

7. Conclusion

ALPS is a framework for helping designers in the industry to adopt the asynchronous techniques. Indeed, asynchronous logic offers lot of solutions in terms of low-power, EM Shaping that can be experimented in our framework. ALPS already offers facilities for A-ADC generation, Asynchronous HLS, EM shaping for respecting EMC. Arithmetic and test are now under investigation because this is a requirement for pushing the technology to our industrial partners.

8. References


Securing Integrated Systems against Malicious Transient Faults and Hardware Trojans


Environmental variations push up huge challenges to the design of integrated systems. Perturbation events arisen from environmental or intentional sources are today able to produce transient faults in circuits by temporarily modifying node voltages, provoking soft errors in stored results from system operations. Examples of environment events are alpha particles released by radioactive impurities and more importantly neutrons from cosmic rays. On the other hand, intentional perturbation events are usually produced by optical sources such as flashlights or laser beams, which can maliciously induce transient effects on secure circuits to retrieve their secret information. Such circuit misbehaviors from fault-based attacks provide fundamental information for cryptanalysis methods that are able to break security applications.

Furthermore, in the last decades, another security issue requiring testing solutions has been discussed: the hardware Trojans. In fact, in the increasing process of globalization, electronics companies rely on outsourcing the different design steps of their IC projects in order to minimize fabrication time and costs, and thus enhancing competitiveness. Hence, designs become vulnerable to malicious alterations during any phase of the IC production. Such modifications are called Hardware Trojan (HT). In the last 15 years, the security community has focused their attention on strategies to make IC production less vulnerable to Trojan insertion. For instance, security agencies of some countries have defined a few trustworthy companies for their mission-critical (military, high tech, medical) IC design flow. On the other hand, for other commercial applications, having the whole IC design flow trustworthy may be too costly. Therefore, researchers all over the world are working on developing methods to identify HT insertion in original design.

Related research works in TIMA’s CDSI group are divided into three subjects: on-line testing techniques for detecting malicious transient faults (e.g., bulk built-in current sensors and transition detection techniques); modeling and simulation of transient-fault effects on integrated circuits; and testing techniques for detecting hardware Trojans in integrated circuits.

1. On-line testing techniques for detecting malicious transient faults

Among the several design strategies for detection of transient faults caused by radiation or optical sources, Bulk Built-In Current Sensors (BBICS) offer a promising solution that is perfectly suitable for system design flows based on CMOS standard cells of commercial libraries. BBICS combine the high detection efficiency of costly fault-tolerance schemes (e.g. duplication with comparison) with the low area and power overheads of less efficient mitigation techniques such as time redundancy approaches. Several architectures of BBICS were recently proposed by our group to monitor transient faults induced on integrated circuits by radiation or malicious sources. The proposed sensors detect anomalous transient currents flowing between any reverse biased drain junction and the bulk of circuits perturbed by events. BBICS indeed takes advantage of the fact that such currents are negligible in fault-free scenarios but are much higher than leakage currents flowing through biased junctions during faulty scenarios. A test chip in technology FD-SOI 28 nm has been designed with a new dynamic BBICS architecture (Figure 1a).

2. Modeling and simulation of transient-fault effects on integrated circuits

Several on-line testing techniques for detecting transient faults have been proposed with the intent to design reliable computing systems. These techniques mainly differ in their detection capabilities and in the constraints they impose on the system design. Although these techniques have been cleverly devised in the last years, confident simulations, practical measures, and evaluations of the real detection efficiency of them against transient faults are still not known in the state-of-the-art. Thus, today it is very hard to identify what is the most efficient technique to protect integrated systems. Hence, the design, simulation, and fabrication of integrated-circuit prototypes embedded with the most recent transient-fault detection techniques are essential. Following, prototypes need be tested with, for instance, laser and radiation facilities able to provide data for evaluating and ranking the real detection efficiencies of the techniques. The correlation between simulation and practical results gives important information for the invention of more efficient transient-fault detection techniques and modeling for fault-injection simulation methods.

The cooperation between TIMA, CMP-GC (Gardanne), and LIRMM (Montpellier) allows the use of a laser source to evaluate the different detection techniques highlighted in previous section. A method for evaluation of transient-fault detection techniques has been proposed (Figure 1a), and another takes into account IR drop effects on the modeling of the transient faults.
induced by laser sources.

3. Testing techniques for detecting hardware Trojans in integrated circuits

In order to reduce HT vulnerability of IC design flows, several methods were developed to prevent HT insertion or detect it by checking anomalous conditions and malfunctions. The research in TIMA’s CDSI group aims to detect Trojan insertion on fabrication phase. By considering that designers have access to the whole design before sending it to fabrication, it is possible to obtain a set of information about the optical design, functional behavior, and expected side-channel signals. Therefore, it is possible to compare the expected set of information with the one generated by the device under test. TIMA’s CDSI group has proposed a new efficient BBICS-based technique for detecting HT (Figure 1b), it was the first one to exploit the impedance of the bulk as a side channel.

![Figure 1](image)

**Figure 1:** (a) Figure of proposed simulation-based method for raking transient-fault detection techniques. (b) Results of new HT-detection technique

4. Publications


Low-Power Event-Driven Image Sensors

**Keywords:** CMOS image sensors, event-based image sensor, low-power image sensor asynchronous logic, design methods and tools, design for ultra-low power

**Members:** L. Fesquet, A. Darwish, H. Abbas, S. Basrour

**Cooperations:** CEA-LETI, LPNC, EPFL

**Contracts:** e-BaCCuSS (Persyval), LACIS (ANR)

1. Low-power event-based image sensors

Due to the improved CMOS processes, the charge coupled devices (CCD) are largely supplanted by the CMOS image sensors. Moreover, plenty of studies have been done to improve the CMOS image sensor performances, in term of image quality but also power consumption. Indeed, the power has become a leitmotiv for all the embedded applications including the systems with an embedded camera such as smartphones, sport cams, etc. Although, the power efficiency of the CMOS image sensors has been enhanced during the last two decades, the standard reading architecture of image sensors still requires an analog to digital converter (ADC), which is currently the most consuming part. Therefore, many studies has been provided in order to reduce the impact of the analog-to-digital converter like using a low power ADCs or a common ADC for the entire sensor[1], [2], [3]. Furthermore the classical reading method of the image sensor consists in reading the entire image for each frame. Consequently, this method limits the reading speed especially for high resolution sensor. Besides, every frame reading induces the reading of temporal and spatial redundant information. Hence, the data flow reduction is probably one of the most important approaches for reducing power in CMOS image sensors. This induces studies like [4]. Therefore the asynchronous image sensor approach is one of the most promising alternatives [5], [6]. Even though, several asynchronous architectures have been already studied, the digital part still suffers from difficulties regarding the pixel management and the timing assumptions. Indeed, most of the proposed architectures are conventional synchronous designs and maintain the need of an analog to digital converter and, for the event-based image sensors, an arbiter is required in order to manage the reading requests and the communications between the pixels and the reading system. In order to overcome these two problems, a fully asynchronous event-driven image sensor, which does not need arbiters, has been designed.

![Figure 1: The asynchronous readout architecture](image1.png)

The proposed sensor performs spatial redundancies suppression and thus a data flow reduction in still image and video streaming by only reading pixels with relevant information. In addition, we removed the analog-to-digital converter, and used instead a voltage to time conversion to encode the pixel information. An asynchronous reading system architecture has been devised. Afterwards, an RTL model of the architecture has been simulated using real pictures as testbenches.

![Figure 2: The testbench used to validate the readout system](image2.png)
2. Pixels and Time-to-First-Spike (TFS) encoding

The time-to-first-spike (TFS) concept is bio-inspired and relies on letting the pixel decide whenever information is relevant or not. Once significant information, the latter is sent and later on processed by the reading system. This technique is implemented in the pixel by introducing a 1-level crossing sampling scheme that also acts as an adaption voltage to the light conditions [7]. Therefore, using this technique allows us to transform the classical analog pixel to an event detector. The event-driven pixel is able to fit the asynchronous and event-driven functioning of the reading system.

The event-driven pixel has the same functioning phases of the classical pixel. Firstly, the reset phase which sets all the pixels to the same initial voltage. Secondly, the integration phase, where the pixel photogenerated current integrates the reset voltage. Finally, the pixel information is extracted by the reading system. The behavior of the pixels and the reading system depends on the nature of the image sensor. On one hand, for a classical image sensor, the duration of the integration phase is predefined and set for all the pixels. The duration of this phase is also known as the integration time. By the end of this phase, the last phase is triggered by the reading system that accesses every pixel in order to extract its information represented by a voltage value across the pixel photodiode. This voltage is later on digitized through an analog to digital converter. On the other hand, for an event-driven image sensor, the pixel determines the duration of its integration phase based on its photogenerated current and thus the amount of incident light. In other words, every pixel has its own integration time. Furthermore, for an event-driven pixel, the pixel information is not expressed by a voltage value but rather a time value that represents the integration time of the pixel. Therefore, the analog to digital converter (ADC) is replaced by a time to digital converter (TDC). In this case, replacing the ADC, which is the most consuming device in the image sensor architecture, reduces the power consumption of the system. It is important to note that the beginning and the end of the integration phase is controlled by the pixel itself thanks to its event detection technique. Subsequently, once an event is detected, the pixel starts to send a request towards the reading system.

3. Conclusion

The results obtained with this architecture are really convincing because we got a pretty good image quality. This has been evaluated with the PSNR and the MSSIM of different images.

Moreover, the number iteration to read the entire image is directly related to the number of gray levels and not to the number of pixels. This gives a serious advantage to quickly catch an image. The low-number of iterations to read the image drastically contributes to reduce the power consumption too. Finally, the image processing can also take advantage of such a sampling as it has been shown for the image segmentation [8].

![Figure 3: Functional diagram of two event-driven pixels under two different luminosities. Vref is the reference voltage used to implement the TFS technique; Vph is the voltage across the pixel photodiode; Tint is the integration time; RRTFS is reading request generated by the pixel once relevant information is detected (Vph crosses Vref)](image)

![Figure 4: Picture samples](image)

<table>
<thead>
<tr>
<th>Picture sample</th>
<th>8a</th>
<th>8b</th>
<th>8c</th>
<th>8d</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-SSIM</td>
<td>0.945</td>
<td>0.878</td>
<td>0.957</td>
<td>0.887</td>
</tr>
<tr>
<td>PSNR</td>
<td>27.31 dB</td>
<td>25.04 dB</td>
<td>27.37 dB</td>
<td>24.21 dB</td>
</tr>
<tr>
<td>% of the original data flow</td>
<td>0.0887%</td>
<td>0.059%</td>
<td>0.11%</td>
<td>0.038%</td>
</tr>
<tr>
<td>Error (%)</td>
<td>3.76%</td>
<td>5.94%</td>
<td>9.23%</td>
<td>6.59%</td>
</tr>
</tbody>
</table>

| Table 1: Final simulation results |

The results obtained with this architecture are really convincing because we got a pretty good image quality. This has been evaluated with the PSNR and the MSSIM of different images.
4. References


