Conception et test des circuits et systèmes numériques à haute fiabilité et sécurité

Giorgio Di Natale

Laboratoire
Informatique
Robotique
Microélectronique
Montpellier

Habilitation à Diriger les Recherches

Giorgio Di Natale

Chargé de Recherche CNRS - Section 7

Conception et test des circuits et systèmes numériques à haute fiabilité et sécurité

Jury:

Matteo Sonza Reorda - Professeur à Politecnico di Torino, Italie

Jean-Luc Danger - Directeur d'études de Telecom ParisTech

Régis Leveugle - Professeur à Grenoble INP

Guy Gogniat - Professeur à l'Université de Bretagne-Sud

Bruno Rouzeyre - Professeur à l'Université de Montpellier II

Lionel Torres - Professeur à l'Université de Montpellier II

Marie-Lise Flottes - Chargé de Recherche CNRS

LIRMM 161, rue Ada Montpellier, 34095 **T** +33467418501 **F** +33467418500 giorgio.dinatale@lirmm.fr

Table of Contents

Chapter I: Summary 5

1. Curriculum Vitae 6

1.1. Personal Information 6

1.2. Cursus 6

1.3. Research Interests 6

1.4. Summary of the hot points 7

2. Summary of scientific activities 8

2.1. Preamble 8

2.2. Current research activities 8

2.3. Students 11

2.4. Scientific Projects 11

2.5. Teaching activities 13

2.6. Cooperations 14

2.7. Dissemination of knowledge 15

2.8. Publications 16

Chapter II: Details 18

3. Research activities 19

3.1. Memory BIST and BISR (Master thesis) 20

3.2. Software Implemented Hardware Fault Tolerance (PhD Thesis) 21

3.3. Memory Test (Post-Doc at Politecnico di Torino, Italy) 23

3.4. Programming by Contracts (Post-Doc at Politecnico di Torino, Italy) 24

3.5. Reliability of the AES (Post-Doc at CNRS) 25

3.6. Manufacturing Test for Secure Devices 30

3.7. Fault Attacks 47

3.8. Test of 3D-Stacked Integrated Circuits 51

3.9. Reliability of Microprocessor-based Systems 53

4. Students 55

4.1. Master students 55

4.2. PhD Students 56

4.3. PostDoc Students 60

5. Teaching activities 62

6. Funded Projects 64

7. Cooperations 70

8. Dissemination of knowledge and scientific excellence 72

Chapter III: Perspectives 76

9. Perspectives on Security 78

9.1. Asset Attacks 78

9.2. IP Attacks 79

9.3. Tampering Attacks 80

10. Perspectives on Test 81

11. Perspectives on Dependability 82

Chapter IV: Publications 84

12. Book chapters 85

13. Journals 85

14. Conferences, Symposium, Workshops, Presentations 86

15. Patent 91

Chapter V: Selection of 5 best papers 93

Chapter I: Summary

1. Curriculum Vitae

1.1. Personal Information

Name:	Giorgio DI NATALE
Date and Place of Birth:	10 February 1975, Torino (Turin, Italy)
Nationality:	Italian
Personal address:	5, rue du Lauzas, 34380 Mas De Londres, France
Current position:	“Chargé de Recherche 1ère classe”, CNRS
Work address:	LIRMM, UMR 5506, 161 rue Ada, 34392 Montpellier Cedex 5, France
Work phone:	04. 67. 41. 85. 01
Fax:	04. 67. 41. 85. 00
Email:	giorgio.dinatale@lirmm.fr

1.2. Cursus

- 1994: High School degree (Computer Science Technical Institute, score 59/60), Turin, Italy
- 1999: Master degree in Computer Engineering (score *summa cum laude*), Politecnico di Torino, Italy
- 1999: National Engineering habilitation exam, Turin, Italy
- 2003: Ph.D. degree in Computer Engineering, Title: “Software-Implemented System Dependability for Safety Critical Applications”, (score Excellent), Politecnico di Torino, Italy
- 2003-2006: Post-doc position, Topic: “Reliability and Test of Digital Systems”, Politecnico di Torino, Italy
- 2006-2007: Post-doc position, Topic: “Design and Test of Secure Circuits”, LIRMM - Montpellier, France
- 2007: Qualification MCF, Section 61, n° 07261174644
- From 2007: Chargé de Recherche 1ère classe, CNRS

1.3. Research Interests

- Memory Testing
- Digital Testing and Design for Testability
- Fault Tolerance and Reliability
- Computer-Aided Design Tools
- Design, Test and Reliability of Secure Devices
- Hardware Security and Trust
- Test of TSV-based 3D Stacked Integrated Circuits
- Dependability of microprocessor-based systems

1.4. Summary of the hot points

- Co-author of 2 book chapters, 18 international journal papers and more than 90 papers and presentations in international conferences, 1 patent
- Co-supervisor of 12 PhD students, 2 Post-Doc students and more than 30 master students.
- Action Chair of the COST Action IC1204 (TRUDEVICE) on Trustworthy Manufacturing and Utilization of Secure Devices
- Scientific leader (for the CNRS) of the FP7 European Project CLERECO (Cross-Layer Early Reliability Evaluation for the Computing cOntinuum)
- Participation to overall 13 european- and national-funded projects (since 2000)
- Associate Editor of the journal “Information Security Journal: A Global Perspective”
- Guest Editor of the journal “IEEE Design & Test”
- Guest Editor of the journal “IEEE JETTA: Journal of Electronic Testing - Theory and Applications”
- Chair of IEEE Computer Society European TTTC
- Database and Web chair of the TTTC and several test-related conferences
- Vice Chair of the Technical Activity “Hardware Security and Trust” of the IEEE Computer Society TTTC
- Co-Chair of the Technical Activity on "Embedded System Security" of GDR (Groupe de Recherche) SoC-SiP of CNRS
- Member of the program committee of several international conferences and reviewers for several journals
- Participation to the company MoleSystems for the development of a peer-review system
- General Chair of TRUDEVICE’13, Vice-Program Chair of DTIS’14, Program-Chair of DTIS’15, Vice Program Chair of ETS’15, Co-General Chair of ISVLSI’15
- Review Chair of DATE conference (since 2012)
- Publication chair of ETS’12, ETS’13, ETS’14, VTS’13, VTS’14
- Publicity chair of the TTEP
- PC Member of: VTS, ETS, IOLTS, DSD, LATW, DCIS, AQTR, EUC
- IEEE Computer Society Golden Core Member
- "Meritorious Service Award - in recognition of more than 8 years of significant services for TTTC Electronic Media"
- Senior Member of IEEE

2. Summary of scientific activities

2.1. Preamble

I have carried out all my studies in Italy. Moreover, after a PhD in Computer Engineering in the domain of the dependability of digital systems at the Politecnico di Torino (Italy), I pursued 4 years of post-doc research at the same institute in the domain of reliability and test of digital systems. Thanks to cooperations between the Politecnico di Torino and the LIRMM of Montpellier, I had the opportunity to obtain a post-doc position in France. There, in addition to the topics which were already familiar to me (i.e., reliability and test), I had the occasion to explore a new application domain: the secure devices. At LIRMM I have kept on working on test and reliability, with a particular focus on secure devices. My scientific results, students I have supervised, my teaching activities, and in general my research projects directly reflects my career path.

2.2. Current research activities

Research activities I carried on after my nomination as *Chargé de Recherche* deal with the definition of methodologies and tools for the design, the test and the reliability of secure digital circuits and trustworthy manufacturing. More recently, we have started a new research activity on the test of 3D stacked Integrated CIrcuits, based on the use of Through Silicon Vias. Moreover, thanks to the relationships I have maintained after my post-doc in Italy, I have kept on cooperating with Politecnico di Torino on the topics related to test and reliability of memories and microprocessors.

2.2.1. Secure and Trusted Devices

Security is a critical part of information and communication technologies and it is the necessary basis for obtaining confidentiality, authentication, and integrity of data. The importance of security is confirmed by the extremely high growth of the smart-card market in the last 20 years. It is reported in "Le monde Informatique" in the article "Computer Crime and Security Survey" in 2007 that financial losses due to attacks on "secure objects" in the digital world are greater than $11 Billions. Since the race among developers of these secure devices and attackers accelerates, also due to the heterogeneity of new systems and their number, the improvement of the resistance of such components becomes today’s major challenge.

Concerning all the possible security threats, the vulnerability of electronic devices that implement cryptography functions (including smart cards, electronic passports) has become the Achille’s heel in the last decade. Indeed, even though recent crypto-algorithms have been proven resistant to cryptanalysis, certain fraudulent manipulations on the hardware implementing such algorithms can allow extracting confidential information. So-called Side-Channel Attacks have been the first type of attacks that target the physical device. They are based on information gathered from the physical implementation of a cryptosystem. For instance, by correlating the power consumed and the data manipulated by the device, it is possible to discover the secret encryption key. Nevertheless, this point is widely addressed and integrated circuit (IC) manufacturers have already developed different kinds of countermeasures.

More recently, new threats have menaced secure devices and the security of the manufacturing process. A first issue is the trustworthiness of the manufacturing process. From one side, secure devices must assure a very high production quality in order not to leak confidential information due to a malfunctioning of the device. Therefore, possible defects due to manufacturing imperfections must be detected. This requires high-quality test procedures that rely on the use of test features that increases the controllability and the observability of inner points of the circuit. Unfortunately, this is harmful from a security point of view, and therefore the access to these test features must be protected from unauthorized users. Another harm is related to the possibility for an untrusted manufacturer to do malicious alterations to the design (for instance to bypass or to disable the security fence of the system). Nowadays, many steps of the production cycle of a circuit are outsourced. For economic reasons, the manufacturing process is often carried out by foundries located in foreign countries. The threat brought by so-called Hardware Trojan Horses, which was long considered theoretical, begins to materialize.

A second issue is the hazard of faults that can appear during the circuit's lifetime and that may affect the circuit behavior by way of soft errors or deliberate manipulations, called Fault Attacks. They can be based on the intentional modification of the circuit's environment (e.g., applying extreme temperature, exposing the IC to radiation, X-rays, ultra-violet or visible light, or tampering with clock frequency) in such a way that the function implemented by the device generates an erroneous result. The attacker can discover secret information by comparing the erroneous result with the correct one. In-the-field detection of any failing behavior is therefore of prime interest for taking further action, such as discontinuing operation or triggering an alarm. In addition, today's smart cards use 90nm technology and according to the various suppliers of chip, 65nm technology will be effective on the horizon 2013-2014. Since the energy required to force a transistor to switch is reduced for these new technologies, next-generation secure systems will become even more sensitive to various classes of fault attacks.

Based on these considerations, within the group I work with, we have proposed new methods, architectures and tools to solve the following problems:

- Test of secure devices: unfortunately, classical techniques for digital circuit testing cannot be easily used in this context. Indeed, classical testing solutions are based on the use of Design-For-Testability techniques that add hardware components to the circuit, aiming to provide full controllability and observability of internal states. Because crypto-processors and others cores in a secure system must pass through high-quality test procedures to ensure that data are correctly processed, testing of crypto chips faces a dilemma. In fact design-for-testability schemes want to provide high controllability and observability of the device while security wants minimal controllability and observability in order to hide the secret. We have therefore proposed, form one side, the use of enhanced scan-based test techniques that exploit compaction schemes to reduce the observability of internal information while preserving the high level of testability. From the other side, we have proposed the use of Built-In Self-Test for such devices in order to avoid scan chain based test.
- Reliability of secure devices: we proposed an on-line self-test architecture for hardware implementation of the Advanced Encryption Standard (AES). The solution exploits the inherent spatial replications of a parallel architecture for implementing functional redundancy at low cost.
- Fault Attacks: one of the most powerful types of attack for secure devices is based on the intentional injection of faults (for instance by using a laser beam) into the system while an encryption occurs. By comparing the outputs of the circuits with and without the injection of the fault, it is possible to identify the secret key. To face this problem we have analyzed how to use error detection and correction codes as counter measure against this type of attack, and we have proposed a new code-based architecture. Moreover, we have proposed a bulk built-in current-sensor that allows detecting the presence of undesired current in the substrate of the CMOS device.
- Fault simulation: to evaluate the effectiveness of countermeasures against fault attacks, we developed an open source fault simulator able to perform fault simulation for the most classical fault models as well as user-defined electrical level fault models, to accurately model the effect of laser injections on CMOS circuits.
- Side-Channel attacks: they exploit physical data-related information leaking from the device (e.g. current consumption or electro-magnetic emission). One of the most intensively studied attacks is the Differential Power Analysis (DPA) that relies on the observation of the chip power fluctuations during data processing. I studied this type of attack in order to evaluate the influence of the countermeasures against fault attack on the power consumption of the device. Indeed, the introduction of countermeasures for one type of attack could lead to the insertion of some circuitry whose power consumption is related to the secret key, thus allowing another type of attack more easily. We have developed a flexible integrated simulation-based environment that allows validating a digital circuit when the device is attacked by means of this attack. All architectures we designed have been validated through this tool. Moreover, we developed a methodology that allows to drastically reduce the time required to validate countermeasures against this type of attack.

2.2.2. TSV- based 3D Stacked Integrated Circuits Test

The stacking process of integrated circuits using TSVs (Through Silicon Via) is a promising technology that keeps the development of the integration more than Moore's law, where TSVs enable to tightly integrate various dies in a 3D fashion.

Nevertheless, 3D integrated circuits present many test challenges including the test at different levels of the 3D fabrication process: pre-, mid-, and post- bond tests. Pre-bond test targets the individual dies at wafer level, by testing not only classical logic (digital logic, IOs, RAM, etc) but also unbounded TSVs. Mid-bond test targets the test of partially assembled 3D stacks, whereas finally post-bond test targets the final circuit.

The activities carried out within this topic cover 2 main issues:

- Pre-bond test of TSVs: the electrical model of a TSV buried within the substrate of a CMOS circuit is a capacitance connected to ground (when the substrate is connected to ground). The main assumption is that a defect may affect the value of that capacitance. By measuring the variation of the capacitance's value it is possible to check whether the TSV is correctly fabricated or not. We have proposed a method to measure the value of the capacitance based on the charge/discharge delay of the RC network containing the TSV.
- Test infrastructures for 3D stacked Integrated Circuits: testing a die before stacking to another die introduces the problem of a dynamic test infrastructure, where test data must be routed to a specific die based on the reached fabrication step. New solutions are proposed in literature that allow reconfiguring the test paths within the circuit, based on on-the-fly requirements. We have started working on an extension of the IEEE P1687 test standard that makes use of an automatic die-detection based on pull-up resistors.

2.2.3. Memory and Microprocessor Test and Reliability

Thanks to device shrinking and miniaturization of fabrication technology, performances of microprocessors and of memories have grown of more than 5 magnitude order in the last 30 years. With this technology trend, it is necessary to face new problems and challenges, such as reliability, transient errors, variability and aging.

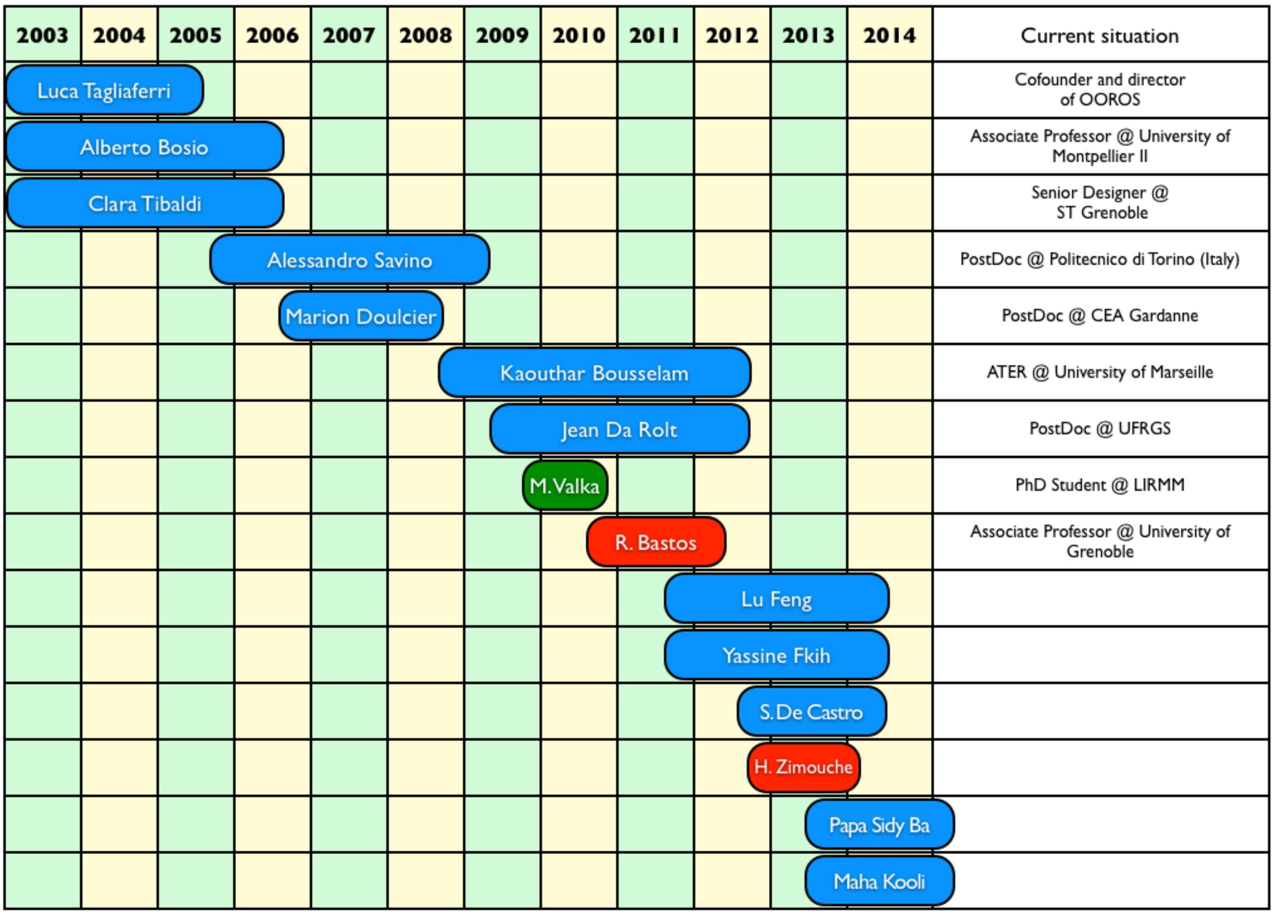
In the last five years I've worked in cooperation with the Testgroup of Politecnico di Torino (Italy) to propose a new method to on-line validate the correctness of the program execution of a microprocessor. The main idea is to monitor a small set of control signals of the processors in order to identify incorrect activation sequences. This approach can detect both permanent and transient errors of the internal logic of the processor.

Concerning the test of memories, we have proposed a new approach to automatically generate test programs starting from a functional description of the possible faults in the memory.

Moreover, we proposed a new methodology, based on microprocessor error probability profiling, that aims at estimating fault injection results without the need of a typical fault injection setup. The proposed methodology is based on two main ideas: a one-time fault-injection analysis of the microprocessor architecture to characterize the probability of successful execution of each of its instructions in presence of a soft-error, and a static and very fast analysis of the control and data flow of the target software application to compute its probability of success.

2.3. Students

After my Ph.D. I have co-supervised 2 post-doc student, 10 Ph.D. students, 1 post-master student, and 32 master students. Table 1 summarizes post-doc (in red), Ph.D. (in blue) and post-master (in green) students in chronological order. Master students are not listed in this table for sake of simplicity. Section 4 of Chapter 2 will describe the work of each student in detail.



<table>
<tr><th>2003</th><th>2004</th><th>2005</th><th>2006</th><th>2007</th><th>2008</th><th>2009</th><th>2010</th><th>2011</th><th>2012</th><th>2013</th><th>2014</th><th>Current situation</th></tr>
<tr><td colspan="3">Luca Tagliaferri</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Cofounder and director of OOROS</td></tr>
<tr><td colspan="4">Alberto Bosio</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Associate Professor @ University of Montpellier II</td></tr>
<tr><td colspan="4">Clara Tibaldi</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Senior Designer @ ST Grenoble</td></tr>
<tr><td></td><td></td><td colspan="5">Alessandro Savino</td><td></td><td></td><td></td><td></td><td></td><td>PostDoc @ Politecnico di Torino (Italy)</td></tr>
<tr><td></td><td></td><td></td><td colspan="3">Marion Doulcier</td><td></td><td></td><td></td><td></td><td></td><td></td><td>PostDoc @ CEA Gardanne</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="5">Kaouthar Bousselam</td><td></td><td></td><td>ATER @ University of Marseille</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">Jean Da Rolt</td><td></td><td></td><td>PostDoc @ UFRGS</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">M.Valka</td><td></td><td></td><td></td><td></td><td>PhD Student @ LIRMM</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="3">R. Bastos</td><td></td><td></td><td>Associate Professor @ University of Grenoble</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">Lu Feng</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">Yassine Fkih</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="3">S.De Castro</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="3">H. Zimouche</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">Papa Sidy Ba</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">Maha Kooli</td><td></td></tr>
</table>

Table 1: Summary of the students

2.4. Scientific Projects

Starting from my Ph.D., I have actively cooperated to national- and european-funded scientific projects. The following list summarizes, for each project, the period, the project type and the type of involvement. Details concerning each project are given in Section 6 of Chapter II.

- 2013-2016: Scientific Leader (for the CNRS) of the European FP7 Project (STREP) called **CLERECO**, which is devoted to the early evaluation of the reliability of complex digital systems based on micro-processors, for both embedded systems and High Performance Computers.
- 2012-2016: Action Chair (i.e., project leader) of the COST Action IC1204, **TRUDEVICE**: “Trustworthy Manufacturing and Utilization of Secure Devices”. This COST action aims at creating a European network of competence and experts on all aspects of hardware security including design, manufacturing, testing, reliability, validation and utilization. The network will

play a key role in developing solutions responding to the hardware security challenges, hence strengthening the position of Europe in the field. I am the coordinator of the whole Action.

- 2012-2015: Participation to the project **MASTER 3D**, which is devoted to the study of 3D Stacked Integrated Circuits. The project is funded by the European CATRENE program.
- 2012-2015: Participation to the project **HOMERE**, which is devoted to the study of Hardware Trojans. The project is funded by the General Directorate for Competitiveness, Industry and Services (DGCIS) and it is sponsored by the "Secure Communications Solutions" competitiveness cluster.
- 2012-2015: Participation to the ANR project **LIESSE**, which is devoted to the study of vulnerabilities of the physical implementation of cryptographic algorithms (CMOS 65, 40, and 28 nm). My group is the leader of the project
- Modeling work laser effects on circuits will be conducted. The resulting models will be used to develop simulators representing physical effects. This project should enable a better understanding of the physical phenomena involved and their experimental application. Its purpose is to propose new principles of security evaluation circuit vis-à-vis these attacks and validate against-measures..
- 2011-2014: Participation to the work package 4 of the project **CALISSON 2**, which aims to unite research efforts in order to improve the security of integrated circuits for the components market which provides security functions. The project is funded by the General Directorate for Competitiveness, Industry and Services (DGCIS) and it is sponsored by the "Secure Communications Solutions" competitiveness cluster.
- 2010-2013: Participation to the Work Packages 2 and 6 (related to test and security) of the project **PROSECURE**, that targets the design and development of an embedded secure microprocessor. This project is funded by the French Languedoc-Roussillon region.
- 2008-2011: Participation to **TOETS** project (European CATRENE CT302) that has the ambition to create a breakthrough in methods and flows used by the test technologies by considering the test in the whole value chain from Design to Application. A strong consortium composed of European Semiconductor industries, Academics and Small and Medium Enterprises has grouped their competences to successfully address this challenge.
- 2007-2010: Participation to the work package 3 of the project **CALISSON**, to enhance the security of electronic devices by developing new design flows in order to reduce the overall design cost and to increase the Time to Market. The project is funded by the General Directorate for Competitiveness, Industry and Services (DGCIS) and it is sponsored by the "Secure Communications Solutions" competitiveness cluster.
- 2004-2006: Participation to **TReDiCo** within the framework of the Protocol for scientific and technological collaboration between the Republic of Italy and Slovak Republic.
- 2001/03: Leader of the Work Package 2 - Task 1 (“BISR for SRAM memories”) of the project called “**TestDOC**: Quality and Reliability of System-on-chip” funded by the Istituto Superiore M. Boella (www.testgroup.polito.it/tdoc)
- 2001/03: Participation to the **GRAAL** project. The goal of this project was the implementation of a tool targeting the automatic generation of highly dependable SRAMs. It has been developed under the project S167P founded by the Italian Ministry of the University and Technological and Scientific Research
- 2000/02: Participation to the framework of the “**Giovani Ricercatori**” (Young Researchers) project at Politecnico di Torino. The goal of the project was the development of new methodologies to increase the dependability of space applications using software techniques.

2.5. Teaching activities

Starting from my Ph.D. studies, I have performed various teaching activities at different levels: engineering students of the Politecnico di Torino and the Engineering School of the University of Montpellier 2, master students of the military school of the University of Torino, students of private institutions, as well as embedded tutorials on specific scientific topics in international conferences. Table 2 summarizes my pedagogical activities. The column dedicated to the time spent for each subject is classified in 3 set: lectures (i.e., “Cours magistraux”), tutorials (i.e., “Travaux dirigés”), and practical work (i.e., “Travaux pratique”).

Subject	Period	Hours			Location
		Lectures	Tutorials	Practical	
Automatic Processes	2005/06	42			University of Torino
	2004/05	42			
Operating Systems	2006/07		10	15	Politecnico di Torino
	2002/03		20	30	
	2001/02		20	30	
	2000/01		20	30	
	2013/14	12			University of Montpellier 2 (UFR)
	2012/13	24			
	2011/12	12			
	2007/08	12		15	
	2005	60		40	Private institution (ENAIP Torino)
	2004	16		16	Private institution (ACME Consulting Torino)
Programming Languages	2005/06		20	30	Politecnico di Torino - C
	2004/05		10	15	
	2003/04		10	15	
	2002/03		10	15	
	2001/02		20	30	
	2000/01		10	15	
	2013/14	15		45	University of Montpellier 2 (Polytech) - C, ASM
	2012/13		40	30	
	2011/12		40	45	
	2010/11		40	60	
	2009/10		40	60	
	2008/09			80	
	2005	50	50	50	Private institution (ENAIP) - JAVA
	2003	10	15	15	Private institution (ACME) - Visual Basic
	2003	15		15	Private institution (CTS Ivrea) - VHDL
	2002	10	15	15	Private institution (Mezzelani Rome) - C++
Databases	2012/13	12			University of Montpellier 2 (Polytech)
	2005/06		10	15	Politecnico di Torino
	2004/05		10	15	
	2001/02		10	15	
	2000/01		10	15	
Digital System Testing	2012/13	12			University of Montpellier 2 (Polytech)
	2006/07	15	10		Politecnico di Torino
	2009	6			Master SISA - Gardanne
	2009	6			International Conferences

Table 2: Summary of the teaching activities

2.6. Cooperations

Table 3 summarizes the main cooperations I had since I started my PhD. I showed only cooperations that led to either a publication, or a common research or networking project.

			Memory Test	µProcessor Test	Reliability	Security	3D Test	Dissemination of knowledge
UNIVERSITIES	Politecnico di Torino	Paolo Prinetto	✓	✓	✓			
		Alfredo Benso	✓	✓	✓			
		Silvia Chiusano	✓					
		Stefano Di Carlo	✓	✓	✓			
		Angelo Serra		✓				
		Matteo Sonza Reorda						✓
	UBS	Guy Gogniat						✓
	TIMA	Paolo Maistri						✓
	Paderborn University	Sybille Hellebrand	✓					✓
	Slovak Academy of Science	Elena Gramatova	✓					
	University of Tehran	M. Hosseinabady			✓			
		Z. Navabi			✓			
	University of Passau	Ilia Polian				✓		✓
	TU Delft	Said Hamdioui				✓		
	KUL	Ingrid Verbauwhede				✓		
	ENMSE	Jean Max Dutertre				✓		
COMPANIES	Siemens	Monica Lobetti Bodoni	✓					
	CEA	Pascal Vivet					✓	
	Yogitech	Riccardo Mariani		✓				
	Mentor	Schloeffel Juergen					✓	
	DGA	Denis Real				✓		

Table 3: Summary of cooperations

2.7. Dissemination of knowledge

Executive and Organizing committees

- TRUDEVICE Workshop: General Chair (2013)
- Design and Test of Integrated Circuits (DTIS): Vice-Program Chair (2014) and Program Chair (2015)
- Design, Automation and Test in Europe Conference (DATE): Review Chair (from 2012)
- VLSI Test Symposium (VTS): Publication Chair (from 2012), Publicity and Web Chair (from 2006 to 2013)
- European Test Symposium (ETS): Vice-Program Chair (ETS'15), Publication Chair (from 2012)
- Latin American Test Workshop (LATW): Publicity Chair (from 2011)
- South European Test Seminar (SETS): General Chair (2007)

Program committee and reviewer

- Associate Editor of the journal: “Information Security Journal: A Global Perspective”
- Guest Editor of the journal “IEEE Design & Test”
- Guest Editor of the journal “IEEE JETTA: Journal of Electronic Testing - Theory and Applications”
- Reviewer for the following Journals: IEEE Transaction on VLSI, IEEE Transaction on Computer, IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Embedded Computing Systems, Journal of Cryptographic Engineering, IEEE Journal of ELectronic Testing - Theory and Applications, IEEE Transactions on Circuits and Systems, Microprocessors and Microsystems, IET Computers & Digital Techniques, International Journal of Communications, Network and System Sciences, IEEE Design and Test of Computers
- Program Committee: DATE (from 2008 to 2011), LATW (from 2012), VTS (from 2007), IOLTS (from 2010), ETS (from 2007), DSD (from 2009), DCIS (from 2006), AQTR (from 2004), EAC (from 2014)
- Reviewer for the following conferences: DAC (2013), ITC (from 2008)

GDR SoC-SiP

- Co-Chair of the Technical Activity on "Embedded System Security" of GDR (Groupe de Recherche) SoC-SiP of CNRS, from 2009 to 2013.

TTTC

- Chair of the European "Test Technology Technical Council" (www.etttc.org) of IEEE Computer Society (from 2014)
- Vice-Chair of the European "Test Technology Technical Council" (www.etttc.org) of IEEE Computer Society (2010-2013)
- Chair of the Database Group of the "Test Technology Technical Council" (TTTC) of IEEE Computer Society (from 2012)
- TTTC Test Technology Educational Program (TTEP): Publicity Chair (from 2012)
- Vice-Chair of the Technical Activity on "HARDWARE SECURITY AND TRUST" of IEEE Computer Society TTTC (from 2011)
- Web Master of the "Test Technology Technical Council" (tab.computer.org/tttc) of IEEE Computer Society (from 2004)

Awards and Certificates

- Best paper (Transaction on Computer), awarded by a movie published at “Computing Now” (http://www.computer.org/portal/web/computingnow/1211/whatsnew/tc)
- "IEEE Computer Society Golden Core Member" (2011)
- "Meritorious Service Award - in recognition of more than 8 years of significant services for TTTC Electronic Media" (2007)
- "Certificate of Appreciation from IEEE Computer Society for serving as TTTC Webmaster in 2006/2007" (2007)
- "Certificate of Appreciation from IEEE Computer Society for serving as TTTC Webmaster in 2004/2005" (2005)

2.8. Publications

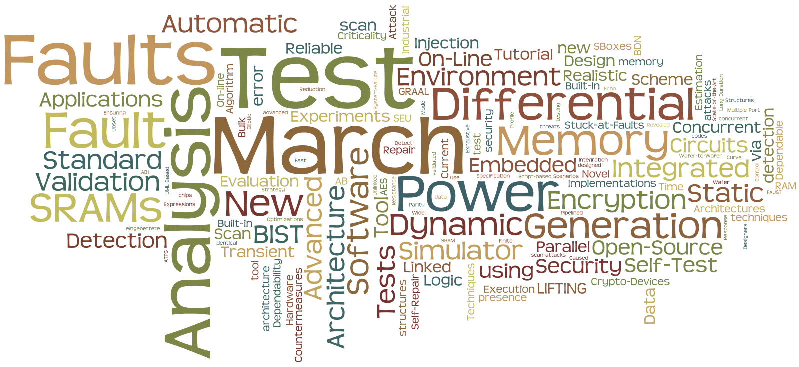
Table 4 summarizes the number of my publications for each year, classified by book chapters, journal papers (with review process), papers published in official proceedings (coming from conferences, symposia or workshops with review process), and presentations given in national and international events without official proceedings.

	Book	Journal	Proceedings			Presentations					Total
Year	Chapter		Conference	Symposium	Workshop	Invited	Workshop	Tutorial	Poster	Demo	
2000	0	0	2	0	2	0	0	0	0	0	4
2001	0	1	2	2	2	0	0	0	0	0	7
2002	0	1	2	1	0	0	0	0	0	0	4
2003	0	2	1	3	1	0	0	0	0	0	7
2005	0	0	2	1	2	0	0	0	0	0	5
2006	0	0	3	5	2	0	0	0	0	0	10
2007	0	1	0	2	1	0	3	0	0	0	7
2008	0	2	1	5	1	0	5	0	0	2	16
2009	0	1	0	0	1	0	0	2	0	0	4
2010	1	1	0	3	0	0	2	1	0	2	10
2011	1	1	1	3	2	0	1	0	0	0	9
2012	0	2	0	3	1	0	4	0	1	0	11
2013	0	5	2	3	3	2	6	0	0	0	21
2014	0	1	1	0	0	0	0	0	0	0	2
Total	**2**	**18**	**62**			**35**					**117**

Table 4: Summary of publications

The complete list of publications is given in Chapter 4. The most cited publications are shown in the following list, leading to an H-index of 15:

1) [J2] --> 48 citations
2) [S5] --> 37 citations
3) [W1] --> 34 citations
4) [C1] --> 34 citations
5) [S1] --> 31 citations
6) [C7] --> 27 citations
7) [S23] --> 22 citations
8) [W2] --> 22 citations
9) [J4] --> 20 citations
10) [S3] --> 19 citations
11) [S18] --> 17 citations
12) [C5] --> 16 citations
13) [S14] --> 15 citations
14) [S7] --> 15 citations
15) [J3] --> 15 citations



Chapter II: Details

3. Research activities

This section summarizes the research activities I carried out starting from my master thesis in 1999.

Research activities at Politecnico di Torino

Since 1999, I worked in the area of digital systems dependability for safety-critical applications at the Politecnico di Torino (Italy), in cooperation with Prof. Paolo Prinetto's research group. His research activity mainly focused on the definition of new methodologies and the implementation of tools able to improve the development of highly dependable systems, at different levels: for basic digital components, for systems on chip, up to microprocessor-based systems. My research activity, developed during 1 year of master thesis, plus 3 years of PhD and 4 years of PostDoc focused on fault tolerance, reliability and test of digital systems. In particular I worked on the following topics:

- Definition of functional fault models for memories RAM and automatic generation of test sequences (Sections 3.1 and 3.3);
- Software Implemented Hardware Fault Tolerance methods (Section 3.2);
- Implementation of a software techniques based on the "Programming by Contract" paradigm for the protection of the application data (Section 3.4).

Research activities at LIRMM

Starting from December 2006 I started working at LIRMM by focusing mainly on the security of hardware devices.

In the last decade, integrated systems are being increasingly deployed in many security-critical infrastructures such as sensitive governmental organizations, military, and financial/banking systems, where the impact and consequences of attacks could be catastrophic. Several types of attacks have been proposed in literature. Among the most known attacks in literature, we have focused on all aspects of the security that either impact or influence the manufacturing testing, or that require the same skills and knowledge strictly related to test and reliability. In particular we worked on the following topics:

- Reliability of the AES (Section 3.5);
- Manufacturing Test of Secure Devices (Section 3.6);
- Fault attacks (Section 3.7)

Besides the activities on hardware security, we have recently addressed the new challenges related to the test of 3D-SIC (Stacked Integrated Circuits).The stacking process of integrated circuits using TSVs (Through Silicon Via) is a promising technology that keeps the development of the integration more than Moore's law, where TSVs enable to tightly integrate various dies in a 3D fashion. The problem of testing 3D-SIC and some solutions are described in Section 3.8.

Finally, in cooperation with the Politecnico di Torino, we propose a new method to on-line validate the correctness of the program execution of a microprocessor, as well as a methodology based on microprocessor error probability profiling that aims at estimating fault injection results without the need of a typical fault injection setup. This activity is described in Section 3.9.

3.1. Memory BIST and BISR (Master thesis)

During my master thesis I explored an architecture able to increase the reliability of a memory, based on self-repair features. The process of repairing a RAM can be divided into several steps. In a first phase, a test algorithm is executed on the memory array. If a fault is detected, it is necessary to locate it (diagnosis) and to allocate redundant memory space to replace the faulty cell. When these operations are built-in the RAM architecture, the steps are named: BIST (Built-In Self-Test), BISD (Built-In Self-Diagnosis), BIRA (Built-In Redundancy-Allocation), BISR (Built-In Self-Repair).

I proposed an innovative architecture for SRAM, characterized by BISR capabilities based on cell-only redundant space allocation at the user level. The memory is not electrically repaired, but spare cells replace faulty ones, using an on-line address re-mapping scheme. The repair process is transparent to the user, and is independent from the memory physical implementation. Moreover, the self-repair architecture is coupled with an ad-hoc defined on-line transparent BIST algorithm, thus implementing a BISTAR (Built-In Self-Test and Repair) approach. The on-line BIST is therefore executed concurrently with the memory normal behavior, and is able to detect the appearance of a wide range of faults, including coupling faults, usually not detectable during end-of-production or power-up tests.

The conceptual idea underlying the proposed approach is to couple an on-line transparent BIST algorithm with a “functional self-repair” architecture in the same BISTAR logic. “Functional self-repair” means that a faulty cell must be replaced by a spare one using an address re-mapping scheme. The BIST part of the logic executes an on-line test, based on a linear algorithm, to detect single stuck-at, transition, coupling, and address faults. Fig. 1 is a conceptual view of the BISTAR architecture. The self-repair logic is based on a CAM used to re-map the address of the faulty cells. The BISTAR controller is in charge of executing the test algorithm and controlling the repair procedures.

The BISR strategy aims at keeping constant the memory storing-capability seen by the user. Faulty cells are functionally replaced by spare ones via a dynamic on-the-fly reconfiguration of the memory-addressing space. From an external user point of view, the memory has a nominal addressing space of N cells, of m-bits each. The actual memory module, instead, has an effective storage capacitance of N+K cells. To optimize the allocation of the redundant memory space, the approach is based on a cell-only repair strategy: when a fault is detected in a cell, instead of repairing an entire row or column, only the faulty cell is re-mapped on a spare one.

Address re-mapping is achieved by a K-lines CAM. In particular, the i^{th} line of the CAM stores the address of the i^{th} faulty cell, that is replaced by the first i^{th} spare cell. This solution allows reducing the area and the routing overhead. Instead of using an additional register into the CAM in which is stored the address of the redundant cell, the association between the line position and the redundant cell is hardwired. Whenever a cell of the memory is accessed, its address is first looked up in the CAM. Two cases can occur:

- If it has been previously detected faulty (or is currently a cell under test), its address has been stored in the CAM. Then, when accessed, the CAM reacts with a hit, and outputs the address of the replace cell, and a proper multiplexer routes it to the memory array. Any operation on the faulty cell is thus performed on its replacement
- If a spare cell does not currently replace the target cell, its address, not being stored in the CAM, is directly transferred to the memory array.

During testing, the cell under test is isolated by replacing it with a spare one: the original content is copied into the spare cell and the CAM content updated for address re-mapping. The test algorithm is then executed on the cell. If no faults are detected, the original content is restored and its re-mapping address in the CAM removed.

This work and its extensions are published in [J1], [J2], [J4], [C1], [C3], [W1], [W2].

3.2. Software Implemented Hardware Fault Tolerance (PhD Thesis)

The PhD thesis has been carried out in the field of safety critical applications that require high dependability. The work focused on the definition of software techniques that guarantee the correctness of the system (both hardware and software) even in presence of faults.

Electronic systems used in military, avionics and aerospace require high reliability and availability. Fault-tolerance has always been an essential attribute of these systems to keep them operational in harsh environments. For example, electromagnetic interference, power glitches and radiations can cause transient faults in electronic systems. Such faults can cause abnormal behavior of computer systems. For example, in radiation environment, alpha-particles, cosmic rays and solar wind flux can cause a Single Event Upset (SEU), which is one of the major sources of bit-flips in digital electronics. A bit-flip is an undesired change in the state of a memory cell; a SEU can cause the state of a memory cell to change from 0 to 1 or 1 to 0, or, in combinational circuits, e.g., an arithmetic logic unit, can lead to incorrect computation results. Besides, devices miniaturization, increasing clock frequencies and the introduction of microprocessors into electrically active environments increase the incidence of SEU also in every day life environments.

Commercial components are usually designed to function in an environment different from that of safety critical applications, thus without fault tolerance capability. If commercial components have to be used for critical applications with no change in hardware, fault tolerance should be provided through software techniques. Software Implemented Hardware Fault Tolerance (SIHFT) detects or tolerates faults in the hardware by software method without any dedicated hardware for error detection or fault tolerance. The benefit of employing SIHFT is that we can improve the availability of the system using the existing design of the hardware available in the market.

To understand the behavior of a computer-based system affected by a SEU when software is running, we have to model and define the errors that occur during program execution. A program can be considered as a sequence of instructions, and the execution of the program can be viewed as executing instructions in a desired sequence. For a more precise description, we define a basic block as a sequence of instructions without any branching inside or outside except for the last instruction; then, a program can be represented by a program graph, which consists of basic blocks and directed edges connecting the basic blocks. If the correct execution sequence in the program graph is broken, it is a Control Flow error. If the information stored in memory is corrupted, it is a Memory error. For example, one of the control flow errors is a branch creation; the correct execution sequence among basic blocks is broken. An example for memory error is the case in which the content of a variable is changed because of a bit-flip.

During my PhD, I developed several innovative SIHFT techniques for the control flow checking and for errors in the memories:

- Reliable C/C++ Code Compiler for dependable applications (RECCO), to check memory errors. The technique is based on a C/C++ Source-to-Source Compiler able to increase the dependability properties of a given application. The adopted strategies are based on code re-ordering and variable duplication/triplication. The approach can be applied to any C/C++ source code, and introduces code modifications that are transparent to the original program functionality. Moreover, it is portable to any platform. The RECCO tool, which fully automates the process, allows the user to trade-off between the level of dependability improvement and the performance degradation due to the code modification;
- A methodology to compute the criticality of variables in a software application. Instead of resorting to time consuming fault injection experiments, the proposed solution is based on the run/time analysis of the variables' behavior logged during the execution of the application under different workloads;
- A detailed error analysis and classification of the behavior of an open-source router, when affected by SEU. The performed experiments allow identifying the most critical router variables according to their impact on system dependability and to validate the strategies employed in the RECCO tool to analyze a C software;

- Control Flow Checking via Regular Expressions, to check the control flow of a program. The check has inserted at source-code level using a signature methodology based on regular expressions. The signature checking is performed without dedicated watchdog processor but resorting to inter-process communication (IPC) facilities offered by most of the modern Operating Systems;
- A static executable code analysis methodology able to compute, depending on the target microprocessor platform, the upper-bound probability that a given application incurs in a Control Flow Error;
- Interposition agents to "wrap" the application software and transparently code all the communications between the application and the surrounding hardware and software environment.

The results of the works carried out during my PhD thesis have been published in the papers [J3], [C2], [C5], [C6], [C9], [S1], [S4], [S5], [S9], [S12], [W3], [W4], [W5], [W7], [P1] referenced in the Publication list. Moreover, part of the work on memory test has been performed in the context of the project "Giovani Ricercatori" (see section 6).

3.3. Memory Test (Post-Doc at Politecnico di Torino, Italy)

The main issue in memory testing is to define comprehensive fault models able to carefully represent the most common defects occurring in the production phase of the chips. Along with fault models, new test algorithms have to be developed. Among the different types of algorithms proposed to test Static Random Access Memories (SRAMs), March Tests have proven to be faster, simpler and regularly structured.

A large number of March Tests with different fault coverage have been published; most of them have been generated by hand. The rapid grow of the memory production technologies introduce new classes of faults, such as Dynamic Memory Faults, making the task of hand writing test algorithms harder and it may lead to non-optimal results.

Although some hand-made March Tests to deal with these new faults have been published, the problem of comprehensive automatically generating March Tests for memory, for classic and new fault models, also easy to extend to user-defined models, was not yet addressed when I started my post-doc.

I proposed a new approach to automatically generate March Tests, starting from a formal model to represent faulty behavior in a memory that allows treating the most important classes of memory faults (Dynamic Faults, Static Faults and also Linked Faults). The formal model is based on Functional Fault Model that is a deviation of the memory behavior from the expected one under a set of performed operations. The memory is modeled resorting to a digraph where nodes represent the memory states whereas arcs represent read and write operations. The automatic generation is based on a visit of the graph, without resorting to exhaustive search. Experimental Results show that newly generated march test can reduce the test complexity, and therefore the test time with respect to the state of the art memory tests published before 2005.

The results of the works carried out have been published in the papers [J5], [J6], [J7], [C4], [C7], [C8], [C10], [S2], [S3], [S7], [S8], [S11], [W8], [W9], [P3], [P4] referenced in the Publication list. Moreover, part of the work on memory test has been performed in the context of the project “TestDOC” (see Section 6).

3.4. Programming by Contracts (Post-Doc at Politecnico di Torino, Italy)

In this field we developed a C++ library called PROMON that encapsulates software techniques to intercept faults that may occur during the execution of the application and, block the execution; the innovative aspect of the approach is that the implemented methodology relies on the principle of Programming by contract, and on the use of common assertions, pre and post-conditions, to ensure that the code follows its expected behavior.

The principle of Design by contract affirms that the interface among the different software modules of a system must be regulated by precise specifications, similar to the human contracts: the contract has to cover the obligations (preconditions), the benefits (post conditions) and the consistence among the limits (invariant).

Pre and post-conditions can be manually setup by an expert programmer or can be automatically extracted from the analysis of the behavior of each variable during a set of fault-free executions of the application. Pre and post conditions are extracted in three phases:

1. Code instrumentation: in the first step the source code of the application is instrumented so that a set of selected critical variables are "redefined" so that, during the software execution, their behavior can be traced on a log file. Obviously all the variables can be redefined but this would in a real case cause an unacceptable overhead.
2. Golden executions: in this phase the user has to run the application with different workloads. During each execution the value of each protected variable is logged for later analysis. The choice of the workloads to apply in order to create the logs, from which the assertions will be extracted, is a very critical task. In general, the more workloads are used, the more the extracted assertions will be precise and less probable to generate "false negatives" (errors not recognized as such);
3. Assertion extraction: in the last phase, all the log files are analyzed and, for each variable, a set of assertions is extracted. In this phase the user can also provide PROMON with a set of "user-defined" assertions, maybe difficult to extract but known as true by the programmer.

At that point, the value of each protected variable is validated, at run-time, using the extracted assertions; if PROMON finds any kind of violation an exception is raised and the execution is stopped. The experiments showed that the technique results in a significant increase of the benchmarks reliability; on the other hand the time overhead introduced by the extra computation can increase rapidly depending on the number of the monitored variables.

The results of the works carried out have been published in the papers [C6], [W5], [W6] referenced in the Publication list.

3.5. Reliability of the AES (Post-Doc at CNRS)

Standard cryptographic functions such as the Advanced Encryption Standard (AES) are today implemented in a wide range of devices targeting various application domains with security requirements. In addition to the inherent property of these devices, allowing storage and transmission of sensitive information across insecure networks, many applications require high reliability for guarantying a proper digital security. Consequently, as other parts of the system, crypto-cores must be carefully designed in order to provide reliable processing of sensible data. Design for on-line testability of such cores prevents structural failures to cause loss of service and compromise the security.

Fault detection and tolerance schemes for various implementations of cryptographic algorithms have been recently considered. Mainly, two approaches have been developed: based on information redundancy (e.g. the use of codes) or functional redundancy.

All the techniques based on codes add some bits to the original data word in order to check its validity. The main issue in these approaches is the prediction of the value of the code on an output, given the input value and the executed operation. For instance, the prediction of a parity bit is almost straightforward for the ShiftRows, MixColumns and AddRoundKey operations performed in the AES because these transformations are either linear or they just perform some bit permutations. Conversely, the prediction of the parity bit is not trivial for the SubBytes operation performed by the so-called S-Boxes. As a consequence, the parity prediction requires larger circuitry. Solutions based on parity codes lead to an overhead of about 20% and high single fault detection. However they are not effective in case of multiple faults or single faults that lead to an even number of errors. Other solutions based on the use of more complex codes such as CRC or systematic nonlinear robust codes lead to higher fault coverage in case of multiple faults but at the expense of a significant area overhead (> 60%).

Functional redundancy can be used whenever encryption and decryption modules are implemented on the same circuit. Each encoding phase is followed by a decoding and compare phase in order to check if the resulting decoded text matches with the initial plaintext. A similar procedure is employed when the circuit is used for decoding a cipher-text.

Conversely to most of the previously proposed approaches that focus on the S-Boxes only (dominant component, counting up to 75% of the circuit area), we proposed a low cost self-test architecture for detecting single and multiple faults in most of the AES hardware. The form of testing is accomplished using duplication and comparison. The main idea is to implement the datapath in such a way that several identical blocks can be defined. With an additional block, online pair wise comparisons of blocks are implemented to check the functionality of the AES hardware. Efficiency and low area overhead are achieved by exploiting the spatial duplication inherent to the parallel implementation of the algorithm.

The technique we proposed is designed for all the AES cores (encryption and decryption) that use 16 S-Box repetitions. We did not consider low-area implementations, where there is only one S-Box at the cost of several clock cycles for completing one encryption/decryption round.

Typical hardware architecture of the AES with 16 S-Boxes is sketched in Figure 2.1. Here, sixteen 8-bit registers feed the 16 identical S-Boxes (S). Shiftrows involves only wires for shifting the bytes of the State, it operates on 128 bits. Four identical MixColumns blocks operate on 32 bits each.

Our goal is to identify a partitioning of the circuit that allows a repetition of identical sub-blocks. These sub-blocks will be compared two-by-two for on-line fault detection thanks to the implementation of an extra sub-block. In the classical architecture depicted in Figure 2.1, ShiftRows unfortunately prevents such a partitioning since it operates on all the 128 bits. However by inspecting the AES algorithm, it can be seen that SubBytes and Shiftrows functions can be switched. We thus propose to perform ShiftRows before SubBytes, and even before loading the registers. Therefore, the datapath can be divided in 4 identical slices that operate on 32 bits each, and that we called RSMA (32-bits Register, 4 S-Boxes, 1 Mixcolumns and 32 xor for the Addroundkey operation).

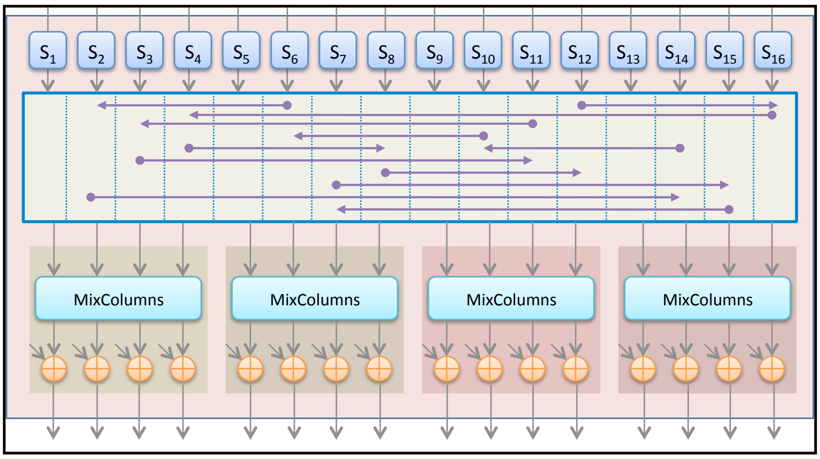


Figure 2.1: Typical AES Datapath

The main idea of the proposed approach is to use one additional RSMA block, and to compare a pair of RSMA blocks at each clock cycle. In particular, at each clock cycle two blocks are fed by the same inputs and the related outputs are compared in order to detect possible faults. Figure 2.2 details the behavior of a part of the circuit where one extra RSMA block has been added. In this figure, LMux(2), LMux(3) and LMux(4) are multiplexers with an additional output that is asserted whenever the two inputs are equal (i.e., a multiplexer with a comparator). Table 2.1 details the signals controlled and observed by the control unit. For instance, when RSMA4 and RSMA3 work together, the UMux(3) let the input I(4) go into the RSMA3. Among the five signals coming from the comparators, only one at a time is considered by the control unit. For example, in the above case, the check(4) signal is verified, i.e., the two related RSMA blocks are checked.

Compared	Um	Lm	To check
RSMA4, RSMA3	1000	11	check(4)
RSMA3, RSMA2	1100	01	check(3)
RSMA2, RSMA1	1110	00	check(2)
RSMA1, RSMA0	1111	00	check(1)
RSMA0, RSMA4	0000	11	check(0)

Table 2.1: Control SIgnals

The scheduling of the comparisons of a pair of RSMA blocks is a very important issue of the proposed method. One AES encryption lasts 10 clock cycles and there are 5 different configurations. Therefore it’s possible to use each of the 5 configurations twice during one encryption. Through the 5 configurations, each RSMA block is compared twice (once with the left block, once with the right block). Thus, if the 5 configurations are activated twice, each RSMA block is compared 4 times during one encryption. A counter is in charge of the test configuration scheduling.

To validate the proposed architecture, we implemented it in VHDL and we synthesized it using Synopsys Design Compiler , and a 130nm CMOS library provided by STM. We considered that all the keys used in the AddRoundKey step (see Annex I) are pre-computed and stored in the circuit. The area of the original circuit is 52961 µm^2 (corresponding to 9660 logic cells) while the area of the proposed architecture is 71357 µm^2 (corresponding to 13084 logic cells and 34.7% of area overhead).

Concerning the efficiency of the proposed architecture with respect to the fault detection, our functional redundancy strategy differs from the classical Double Modular Redundancy (DMR) scheme. A classical DMR architecture allows detecting all the faults (single and multiple) that lead to an error (i.e., a difference at the output of one of the duplicated modules). Starting from the moment of appearance of the fault, the fault latency depends on the inputs applied to the circuit, only. In other words, the fault is detected as soon as the input vector can sensitize the fault and propagate it up to the output of the module (i.e., the input of the comparator between the two modules). Anyway, a system based on classical DMR scheme does not deliver faulty responses without noticing it (unless in case of equivalent faults in the two modules).

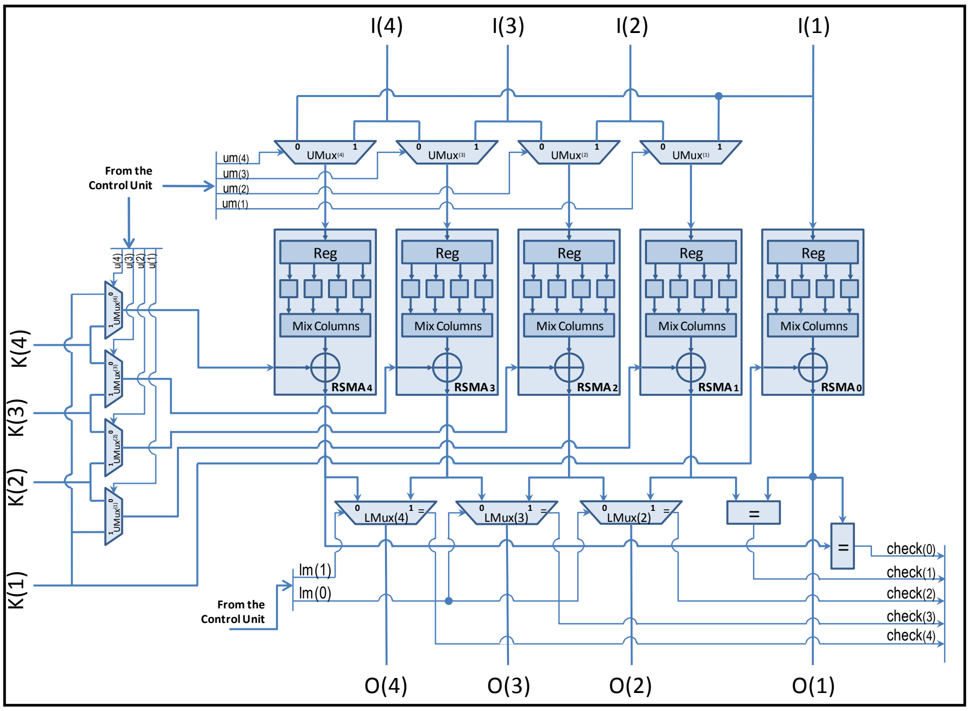


Figure 2.2: AES Architecture with RSMA duplication and comparison

This technique is able to detect any single or multiple faults leading to a wrong RSMA output value (as for the classical DMR) but only when the affected RSMA is compared with another one. Conversely to DMR, the dynamic reconfiguration of the modules leads to a comparison of each module twice every 5 clock cycles. Therefore it can happen that the system produces erroneous responses without noticing it even in presence of a single stuck-at.

We questioned the probability to get an error on the AES output and to not detect it. This probability can be analyzed by computing the probability $P_{err}(f)$ of not detecting an error on the circuit's outputs while a given fault f affects the circuits. For this analysis we focused on single stuck-at faults only.

$P_{err}(f)$ is the probability that the fault f is activated (i.e. sensitized and propagated in such a way that it leads to an error) during at least one of the 6 clock-cycles during which the faulty RSMA is not compared, and it is not activated during the 4 clock cycles when the RSMA is compared. Let denote p_f the probability of activation of a fault f into an RSMA module, i.e., the probability that for a random input pattern the fault is sensitized and the error is propagated to its output. In the hypothesis to have several distinct functional inputs, we can consider that the device is fed by a random source. In addition, the inherent properties of the AES makes that the sequence of input values that are applied to consecutive rounds of the same encryption can be considered as random. Therefore, the probability p_f is equal to the ratio of input vectors that test f over the number of possible input vectors. The number of possible input vectors for the RSMA, is 2^{32}. Since fault simulation cannot be applied in exhaustive way, we split the problem in two parts. From one side, S-Boxes have 8 input bits only, consequently exhaustive analysis is possible and p_f can be obtained for each fault through simulation. Since MixColumns and AddRoundKey are invertible functions, all the errors appearing on the output of the S-Boxes propagate through the functions to the comparator. From the other side, p_f of the MixColumns has been calculated thanks to its modular structure involving 4 identical 8-bit inputs sub-functions (2^8 combinations). Finally, the AddRoundKey operations involve only xor operations and are very easily tested.

For the proposed architecture, the probability that f is not activated during the clock-cycles of comparison is equal to $(1\text{-}p_f)^4$ while the probability that f is activated during at least one of the clock-cycles without comparison is equal to $1\text{-}(1\text{-}p_f)^6$. Finally, it comes:

$$P_{err}(f) = \left(1 - p_f\right)^4 \times \left(1 - \left(1 - p_f\right)^6\right)$$

Figure 2.3 represents $P_{err}(f)$ in function of p_f. Hard-to-test faults ($p_f \approx 0$) and the easy-to-test faults ($p_f \approx 1$) are not those that most likely produce undetected errors. On the contrary, the maximum value (32.57%) corresponds to faults with p_f equals to 0.14.

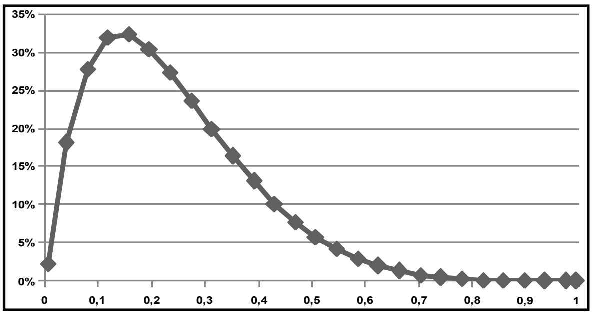


Figure 2.3: $P_{err}(f)$

In order to calculate the error probability of the whole circuit (actually 97% of the circuit, being MixColumns omitted), we fault simulated the Sboxes to determine the distribution of probabilities of activation of the faults. Basically, we calculated how many faults are activated by one test pattern (p_f = 1/256), how many faults are activated by 2 patterns (p_f = 2/256), and so on. Figure 2.4 summarizes, for each probability pf, the number FD(pf) of faults with that activation probability.

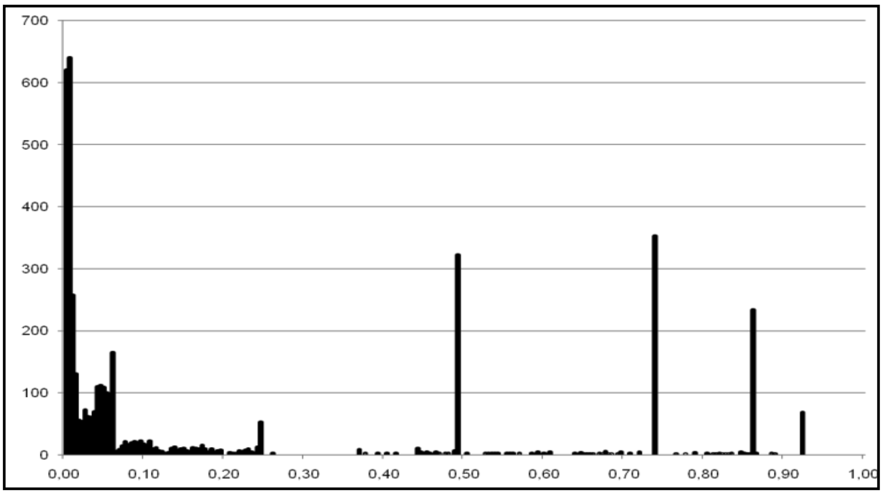


Figure 2.4: $FD(p_f)$

Assuming that each fault has the same probability to appear in the circuit, the overall error probability P_{ERR} of the RSMA is calculated as the weighted average of the values Perr(f) according to the distribution FD(p):

$$P_{ERR} = \frac{1}{\#Faults}\sum_{i=1}^{256}\left\{\left[FD\left(\frac{i}{256}\right)\right] \times \left[\left(1-\frac{i}{256}\right)^4 \times \left(1-\left(1-\frac{i}{256}\right)^6\right)\right]\right\}$$

It comes that PERR is equal to 10.18%, i.e. the architecture has a probability of 89.82% to detect any fault in a single encryption (10 clock cycles). We also analyzed the evolution of this probability based on the number of encryptions. When we perform E encryptions, an RSMA block is compared 4·E clock cycles, while it is not compared 6·E clock cycles. The error probability can therefore be rewritten as follows:

$$P_{err}\left(E,f\right)=\left(1-p_f\right)^{4\cdot E}\times\left(1-\left(1-p_f\right)\right)^{6\cdot E}$$

Considering the fault distribution FD given in Figure 2.5, we can re-calculate the overall error probability P_{ERR} of the RSMA block in function of the number of encryptions (Figure 7). As can be seen, the error probability slightly increases up to 14% for 5 encryptions, while for higher encryption numbers it tends to 0. Namely, for 300 encryptions, the reliability probability is equal to 99.9%.

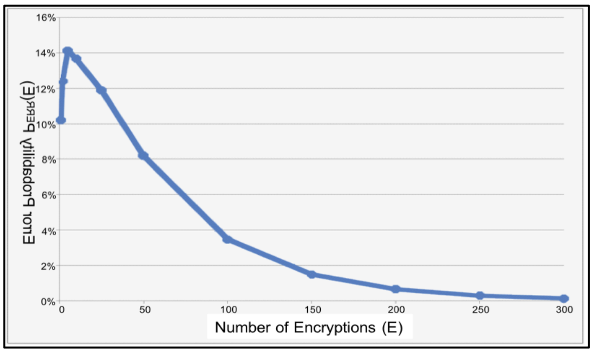


Figure 2.5: Error probability w.r.t. the number of encryptions

To conclude, we proposed a low cost architecture for detecting single and multiple faults in the hardware implementation of the Advanced Encryption Standard (AES) during its mission mode. The solution, based on spatial redundancy, reorders the AES algorithm subtasks. This modification does not influence the actual encryption function and it allows the implementation of 4 identical blocks working on 32-bits each. Thanks to this parallel and duplicated architecture, only one additional 32-bits block is added in the circuit leading to 4 tests per encryption cycle for every block. The solution is very effective in terms of fault latency and fault coverage while keeping the area overhead very low (about 34.7%).

The results of the works carried out have been published in the papers [J8], [S13], [S15], [P6], [p7] referenced in the Publication list.

3.6. Manufacturing Test for Secure Devices

Structural testing is one important step in the production of integrated circuits. Indeed, the fabrication of CMOS devices is not a totally controlled process and some of the manufacturing chips may not work properly. Testing is therefore essential to sort faulty and good circuits and thus ensure the quality of the products. The increasingly test cost of new technologies demands the insertion of test-oriented structures early in the circuit design, which is call Design-for-Testability (DfT). These structures aims at improving the testability (mainly the capacity to detecting the presence of faults), diagnostics, test time and reducing the number of required test pins.

The most common DfT technique is the insertion of scan chains, which increases the observability and the controllability of the circuit's internal nodes, increasing then the testability. Nevertheless, malicious users can use the scan chains to observe confidential data stored in devices implementing cryptographic primitives. Therefore, scan chains inserted in secure ICs can be considered as a source of information leakage. However, testing cannot be simply avoided in secure products for two main reasons: first possible non- tested errors may compromise the system's security and as for any other IC, the test ensures the quality of the product.

Besides the security threat that lies in the scan chains, standard test interfaces such as JTAG and IEEE 1500 can also be maliciously exploited. These test interfaces that initially developed for testing printed circuit boards (JTAG) or System-on-Chip internal modules (IEEE 1500), can be used nowadays for debugging purposes. Easy access to debug ports and module's test structures can be used by hackers to steal the contents of on-chip memories (intellectual property) and to modify the firmware/software so that the device executes a function which was not initially conceived by the designer. In order to protect intellectual property the security of these ubiquitous test interfaces must be improved.

In the last 5 year we have analyzed the weaknesses of standard DfT architectures based on the use of scan chains, and we have proposed new countermeasures to cope with this hazard. The following subsections will summarize our main contributions. The rest of the section is structured as follows:

1. a description of the basic approach the allows successful scan attacks, followed by new attacks we proposed;

2. the countermeasures we have proposed to cope with those attacks. We have investigated solutions based on Built-In Self-Test, on the internal comparison of test and expected responses, the implementation of a smart controller, and the enhancement of the security of the JTAG standard.

3.6.1. Scan Attacks

The insertion of scan chains consists of replacing the flip-flops (FFs) of the design by scan flip-flops (SFFs) and connecting these SFFs into a shift-register, called scan chain. The scan chain is bound to a input pin (scan-in) and to an output pin (scan-out). An extra pin called scan-enable should be added to control the scan chain's data shifting. If the scan-enable is set to 0, the SFFs are connected to the circuit to behave as functionally expected (functional mode). When the scan-enable is set to 1, then the SFFs are connected to the scan chain, and the bit-stream at the scan-in is shifted in while the data stored in the SFFs is shifted out through the scan-out pin.

The attacker may use the shift operation maliciously in order to discover the secret key of a cryptographic algorithm that is stored within the circuit. An attack would consist of the following steps:

1. Reset the circuit;

2. Load the chosen input at the cipher's input;

3. Run part of the encryption (functional mode on);

4. Switch to test mode when the intermediate flip-flops contain data related to the secret and shift out the scan contents containing this confidential information;

5. Analyze the observed contents and try to uncover the secret key. If there is not enough information, repeat the process for another chosen inputs.

In order to reduce the complexity of the procedure, most attacks relies on the so-called differential analysis. This strategy makes use of pairs of cipher inputs (that differentiates for few bits) and calculate the differences (Hamming distances) from the output related to these pairs. This technique allows revealing only the bit that changed from one input to the other, and it removes all involved constant values. All the known scan-based attacks use this principle to collect scan data. In the last years, the literature have seen a succession of papers proposing a new scan attack, followed by a paper proposing the related countermeasure. In this context, we have proposed several scan attacks that showed their effectiveness even in presence scan compression/compaction schemes that were considered (before our paper) an intrinsic countermeasure against scan attacks.

Advanced DfT Structures & Security

Structural test consists in applying test patterns to the circuit under test. These patterns are being derived from the circuit's structure (logic gates netlist) and a fault model (e.g. stuck-at faults). In addition to structural test, DfT approaches are required for improving fault coverage and thus product quality. The most widely used methodology for structured DfT is the so-called scan chain. The circuit's flip-flops are replaced by scan flip-flops and then connected to each other in order to form a shift register (scan chain): the first scan flip-flop in the chain is connected to the scan-in port and the last one to the scan-out port (see Fig. 2.6.a). The scan chain provides full controllability and observability of storage elements and thus of the circuit's internal states. Possibly, sufficient fault coverage is achieved with only some of the flip-flops within the scan chain, leading to the so-called partial-scan design.

We define here three types of scan flip-flops depending on the stored value. This classification is valid for any device with cryptographic blocks and it will help the description of the attack throughout the paper. Independent flip-flops (IFFs) store data that is independent from crypto inputs. Dependent flip-flops (DFFs) store data that depends on crypto inputs but is independent from secret data (e.g. input buffers of the cryptographic block). Secret flip-flops (SFFs) store data that depends on the secret key. An example showing these three types of flip-flops is depicted in Fig. 2.6.b. It contains 4 IFFs, 3 DFFs and 3 SFFs. It must be noted that this classification is only valid for a given time-step during computation. For instance, a FF may contain a datum depending only on the input value at a given instant, while it may contain datum depending on the secret key at another instant. Thus, the attacker should predict the instant when secret is stored in the scan chain, in order to shift out the test data and analyze it to calculate the secret.

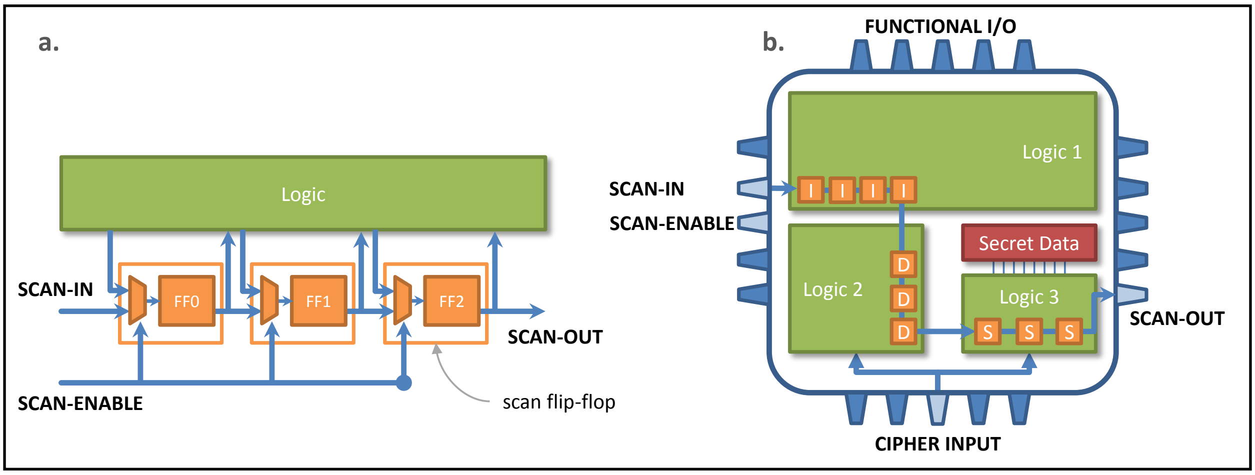


Fig. 2.6: (a) Scan flip-flops in the scan chain; (b) Example of a device with cryptographic block

There are two operating modes in scan designs: functional mode and shift mode. These modes are differentiated by using an extra test signal (scan-enable). In functional mode, the scan design operates within the functional configuration. The shift mode is used to shift test patterns in and shift test responses out. In order to test the circuit, test patterns are loaded from the scan-in while the primary inputs are set accordingly to the test. Then the circuit is switched to functional mode for one cycle to capture the circuit's internal state into the scan chain. Finally, data captured in the scan chain are shifted out through the scan-out port for response observation.

In complex designs a scan chain may contain thousands of sequential cells. Unfortunately, long scan chains have a negative impact on test time due to the required shift operations at every test pattern. In this case, multiple scan chains are implemented requiring as many scan-in and scan-out pins as the implemented scan chains. In order to meet the number of design digital pins, certain methods are used for reducing the number of visible scan chains. Compression is used to reduce the number of bits in test vectors. An on-chip decompressor is then implemented to regenerate the full test vectors to the scan chain inputs from the compressed test sequence. On the scan-out side, the number of scan-out pins is reduced using so-called compaction structures. Compactors are usually implemented using XOR trees containing one or several outputs. If one fault is captured by one scan flip-flop then it propagates through one of the compactor outputs and becomes detectable.

Another structure commonly seen in structural tests is the mask decoder. Its goal is to mask the presence of unpredictable values (called X's) that may corrupt test output data and thus lower fault coverage and diagnosis. These X's are due to uninitialized memories and flip-flops, or bus contention. The mask decoder is fed by test inputs and, based on the input value, it deactivates some scan chains (those that contain an X).

An example of spatial compaction is shown in Fig. 2.7. In this example, the 20 scan flip-flops are distributed over 4 scan chains and form 5 slices. A slice is made of flip-flops belonging to the same rank in the scan chains. In this example the content of the flip-flops within a slice is compacted in a single bit by the response compactor. H[i] is the result of slice i compaction. Hereafter, we assume a single output compactor. From an attacker's point of view this is the worst-case scenario, since observability is reduced to a minimum: all slices' elements are compacted into a single bit. When a multi-output compactor is used, the attacker can simply compute H[i] by XORing the bits on the outputs.

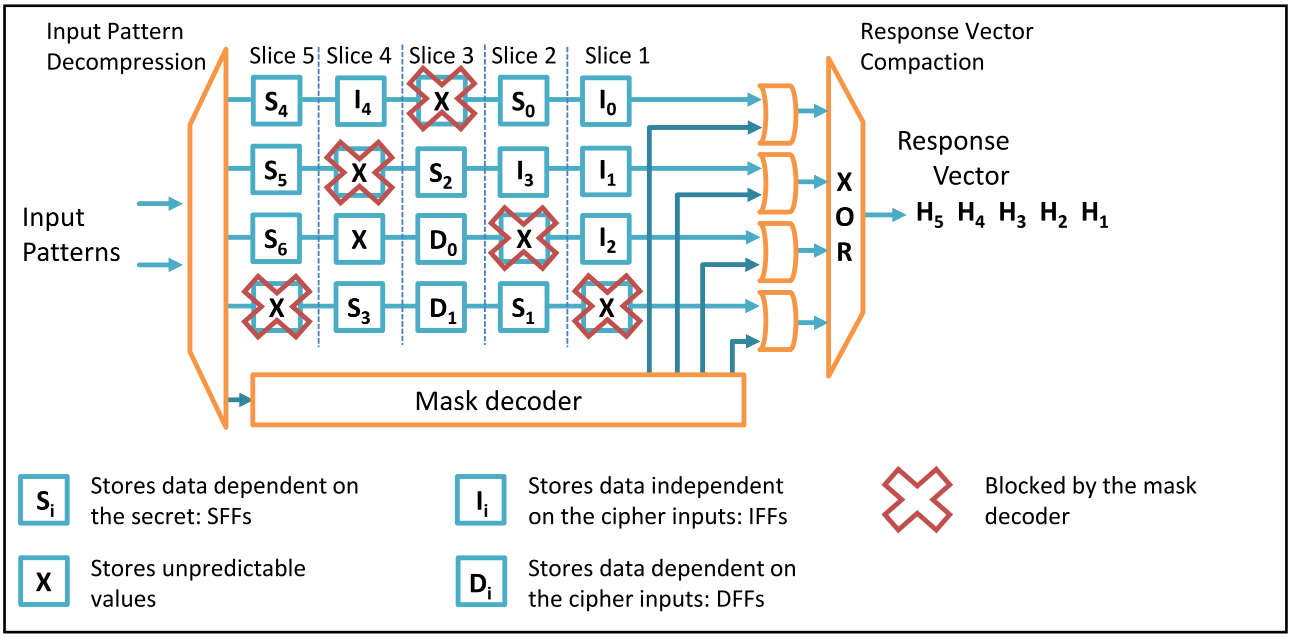

Input Pattern Decompression
Input Patterns
Slice 5
Slice 4
Slice 3
Slice 2
Slice 1
S_4
I_4
X
S_0
I_0
S_5
X
S_2
I_3
I_1
S_6
X
D_0
X
I_2
X
S_3
D_1
S_1
X
Mask decoder
Response Vector Compaction
XOR
Response Vector
H_5 H_4 H_3 H_2 H_1
S_i
Stores data dependent on the secret: SFFs
I_i
Stores data independent on the cipher inputs: IFFs
Blocked by the mask decoder
X
Stores unpredictable values
D_i
Stores data dependent on the cipher inputs: DFFs

Fig. 2.7: Example of circuit with spatial compaction and mask decoder

We shall use the example of Fig. 2.7 throughout the paper for explanatory purposes. While this example is quite simple, it must be noted that the slices contain all possible combinations of various scan flip-flop types (SFFs, DFFs, IFFs).

In a single chain or multiple scan-chains scenario without compaction, values related to secret data are left unchanged in the observed scan-out bitstream. In presence of response compaction, secret-related data (SFFs) compacted with other data, such as data stored in IFFs and/or DFFs. This makes the previously mentioned scan-attacks impossible. The mask decoder also makes the attack more difficult. From the test engineer's point of view, the mask is used to filter the unpredictable values. On the other hand, an attacker that has no knowledge of the DfT structure cannot predict the presence/position of X's. Therefore, when he shifts out the internal states, he is not able to set correctly the mask. In this case, X's may corrupt the test outputs, making the attack impossible. Other issue caused by the improper use of the mask decoder is that it may mask data related to the secret instead of X's and thus only part of the secret related data is observable at the output. The same occurs in case of partial scan designs, where only a subset of flip-flops are inserted into the scan chain and in the case of MISR compaction, where the final signature is the only information delivered to eventual hackers.

To sum up, in the presence of such advanced DfT structures, exploiting test outputs in order to expose the secret is far more challenging than setting scan attacks on single-scan chain designs. However, the work we proposed demonstrates how to set up scan attacks on advanced scan designs, showing how to exploit test outputs, even when only part of the SFFs are observable in the test output.

Definitions and Assumptions

Scan attacks compromise system security because the test infrastructures can be used to observe internal states. The following procedure is used (several times) in the attack to unload the circuit's internal state into the test output.

Procedure 1. Collecting internal states into test output

1. Reset the circuit;
2. Load a chosen plaintext M (message);
3. Run the crypto algorithm until it executes the first operation on the plaintext, based on the value of a secret key, and store intermediate values in SFFs;
4. Switch from normal mode to shift mode;
5. Shift out the scan data;

In order to determine the time required to run the crypto algorithm, the attacker uses the information described in the device datasheet or SPA (Simple Power Analysis), which may help find out the number of cycles. The attacker repeats Procedure 1 for some messages and then analyzes the data observed on the scan-out. The attacker must identify which data in the scan-out stream correspond to the data stored in SFFs. For single-chain scenarios it is very straightforward to analyze the scan-out data. However in the presence of industrial DfT structures it requires special considerations detailed below.

The attack rely on the differential analyses, which assess differences instead of direct values, are well-known in the hardware security community. Several studies using Differential Power Analysis (DPA) or Differential Fault Analysis (DFA) relying on differential values instead of direct values have been validated as methods for compromising the security of hardware implementations. The above has two main advantages: eliminating some issues introduced by spatial compaction and helping the attacker find out which bits of the observed test output bit stream are related to the secret data.

In the context of scan-attack, the attack relies on the analysis of the difference between two test output vectors.

The example of Fig. 2.7 will be used hereafter since it is representative of all possible flip-flop combinations between SFFs, DFFs and IFFs. As seen in Fig. 2.7, H represents the response vector, therefore H[1] is the first element of this vector (corresponding to slice 1) and so on. The equations for all test output bits i are described by Eq. 1-5:

$$H[1] = I_0 \oplus I_1 \oplus I_2 \qquad (1)$$

$$H[2] = I_3 \oplus S_0 \oplus S_1 \tag{2}$$
$$H[3] = S_2 \oplus D_0 \oplus D_1 \tag{3}$$
$$H[4] = S_3 \oplus I_4 \oplus X \tag{4}$$
$$H[5] = S_4 \oplus S_5 \oplus S_6 \tag{5}$$

The differential analysis described in Procedure 2 basically consists in executing Procedure 1 for several pairs of input messages in order to observe the differences in the information stored within the scan chain(s) when the message changes:

Procedure 2. Differential Scan Analysis

```
1.  Execute Procedure 1 with cipher input $M_j$ (message) and observe the test response $H^j$ (an array containing five bits: H[1] to H[5]);
2.  Execute Procedure 1 with cipher input $M_k$ and observe the test response $H^k$;
3.  For each index i of the arrays $H^j$ and $H^k$:
4.      Store in $Diff_{j,k}[i]$ the difference (XOR) between $H[i]^j$ and $H[i]^k$;
```

By repeating Procedure 2 for several pairs of messages (Mj, Mk), the attacker obtains several arrays of differences, hereafter called measured signature (each test response bit i has a signature denoted hereafter Diff [i]):

$$Diff\,[i] = Diff_{0,1}[i]\,||Diff_{2,3}[i]\,||Diff_{4,5}[i]\,||\,Diff_{6,7}[i]\,||\ldots$$

Applying the pair of messages (Mj, Mk) to the example of Fig. 2.7 we obtain Eq. 6-10:

$$Diff_{j,k}\,[1] = I_0^j \oplus I_0^k \oplus I_1^j \oplus I_1^k \oplus I_2^j \oplus I_2^k \tag{6}$$
$$Diff_{j,k}\,[2] = I_3^j \oplus I_3^k \oplus S_0^j \oplus S_0^k \oplus S_1^j \oplus S_1^k \tag{7}$$
$$Diff_{j,k}\,[3] = S_2^j \oplus S_2^k \oplus D_0^j \oplus D_0^k \oplus D_1^j \oplus D_1^k \tag{8}$$
$$Diff_{j,k}\,[4] = S_3^j \oplus S_3^k \oplus I_4^j \oplus I_4^k \oplus X_4^j \oplus X_4^k \tag{9}$$
$$Diff_{j,k}\,[5] = S_4^j \oplus S_4^k \oplus S_5^j \oplus S_5^k \oplus S_6^j \oplus S_6^k \tag{10}$$

Since only cipher inputs differ between the first and second execution of Procedure 1 (line 1 and 2), IFFs are not affected by Mj and Mk and store the same values, thus differences between the values stored in any IFF for any two different messages Mj and Mk amount to 0. It implies that the equations (6)-(10) can be rewritten as:

$$Diff_{j,k}\,[1] = 0 \tag{11}$$
$$Diff_{j,k}\,[2] = S_0^j \oplus S_0^k \oplus S_1^j \oplus S_1^k \tag{12}$$
$$Diff_{j,k}\,[3] = S_2^j \oplus S_2^k \oplus D_0^j \oplus D_0^k \oplus D_1^j \oplus D_1^k \tag{13}$$
$$Diff_{j,k}\,[4] = S_3^j \oplus S_3^k \oplus X^j \oplus X^k \tag{14}$$
$$Diff_{j,k}\,[5] = S_4^j \oplus S_4^k \oplus S_5^j \oplus S_5^k \oplus S_6^j \oplus S_6^k \tag{15}$$

Since Diffj,k[1] is related to a slice that contains only IFFs, there is no input pair that can provoke a difference in that particular output bit (see Eq. 11). By observing the test outputs, the attacker can observe which output bits H[i] never change and deduce that they are only related to IFFs, as the example of Eq. 11.

The cases of Eq. 12 and Eq. 15 correspond to slices with only SFFs and IFFs (the differential analysis eliminated the differences coming from IFFs). The proposed attack (as shown below) allows the attacker to find out which output bits are only related to SFFs and IFFs and retrieve the key related to those SFFs. It is important to remember here that the DfT structure is completely unknown to the attacker, i.e. the attack method is independent of the DfT structure.

The presence of X's can also complicate the attack. In a normal test procedure, applying an appropriate mask eliminates the X's. On the other hand, the attacker has no knowledge on the DfT structure, and then the avoidance of X's is not ensured.

When the proposed procedure fails to identify H[i] values of interest, the attacker must provide new inputs to the device, knowing that these inputs will affect the mask (even if the attacker does not know how the mask is affected).

Proposed Attack (Signature Attack)

The principle of the signature attack is to characterize all signatures (Diff [i]) for a set of input pairs, for all possible key guesses. Since the distribution of the SFFs amongst the slices is unknown to the attacker, this has to be done for all possible subsets of SFFs observable at the output. The characterized signatures must be different so that a measured signature (Procedure 2) corresponds to only one characterized signature. In other words, the measured signature can be generated by only one key and only one subset of observable SFFs. Thus, the signature attack consists in two phases: characterizing all possible signatures (via simulation) and obtaining the measured signature (in the attacked device, via Procedure 2).

Fig. 2.8 depicts the signature simulation process when all SFFs are observable and affect the same test output bit. For each possible subset of observable SFFs a similar table must be simulated. If N is the number of SFFs, then there are 2^N possible observable subsets (and corresponding tables).

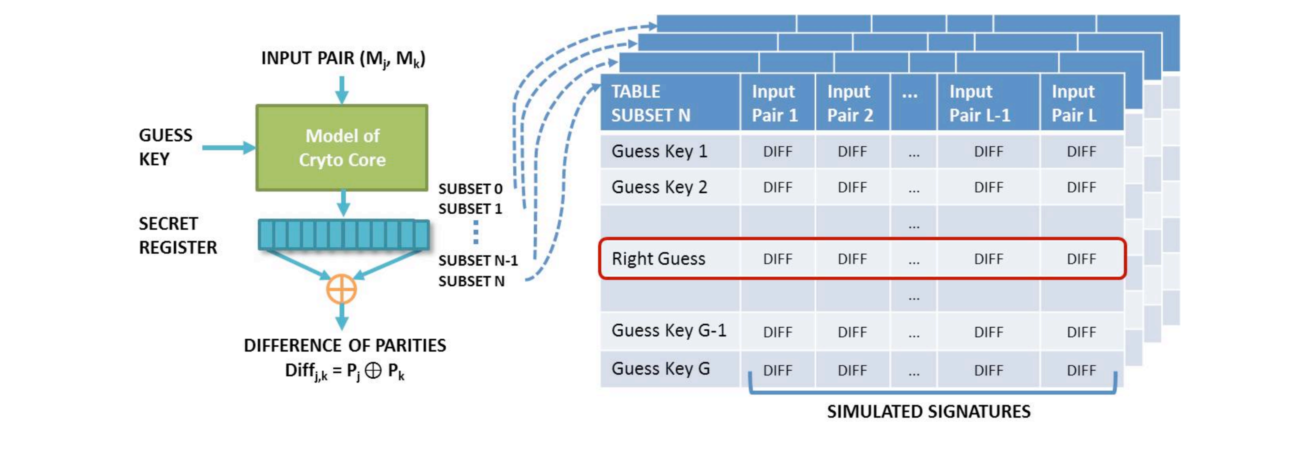


TABLE SUBSET N	Input Pair 1	Input Pair 2	...	Input Pair L-1	Input Pair L
Guess Key 1	DIFF	DIFF	...	DIFF	DIFF
Guess Key 2	DIFF	DIFF	...	DIFF	DIFF
			...		
Right Guess	DIFF	DIFF	...	DIFF	DIFF
			...		
Guess Key G-1	DIFF	DIFF	...	DIFF	DIFF
Guess Key G	DIFF	DIFF	...	DIFF	DIFF

Fig. 2.8: Simulated signatures for possible subsets of observable SFFs

Besides simulating these signatures, simulated signature must be unique, i.e. there are no duplications among all the table lines (signatures). This property (uniqueness) allows the measured signature to match a single simulated signature with only one key and subset table. Obviously, the number of signatures to be simulated is exponentially increased by the number of SFFs and by the number of bits of the key. We have shown that in practice we can use some techniques to focus on small groups of key bits and SFFs at a time, to make feasible the simulation of signatures.

The second phase of the signature attack consists in retrieving the measured signature from the device. For that purpose, the attacker applies the same set of input pairs (Mj, Mk) from the simulation phase (the one with uniqueness property). Then he applies Procedure 2 for each pair, and creates measured signatures. Each output bit stream Hj corresponds to a message Mj. For each pair of messages (Mj, Mk) the attacker calculates the difference between Hj and Hk. After applying some pairs each test output bit H[i] has a measured signature consisting in a series of differences.

Once all measured signatures are obtained, the attacker compares them to the simulated signatures (from Fig. 2.8). If one test output bit H[i] depends only on SFFs and/or IFFs (such as H[3] and H[5]), the measured signature for this slice will match one of the simulated signatures. The matching signature corresponds to the subset of SFFs observed in that test output bit H[i], and reveals the key guess that corresponds to the secret key.

Since the signatures are computed from the SFFs values, this attack works only if the design contains some slices with only SFFs and IFFs. If the SFFs always mixed with DFFs within the slices, the attack fails, since the observed signatures are corrupted by the values stored in the DFFS. We have therefore extended this attack to this case.

Enhanced Attack

If a SFF is compacted along with a DFF (for instance see output H[3], see Eq. 13), then the parity obtained from the corresponding slice cannot be exploited by scan-attacks. However, today's designs certainly contain some DFFs (e.g. input registers) that will be part of the scan chains and are mixed with SFFs. Then, in order to widen the scope of the attack, we proposed an extension that copes with the presence of DFFs.

The principle of the attack cannot be directly extended to the presence of DFFs since the attacker cannot predict (simulate) their value to compute signatures. Therefore, here we show that using two additional identical circuits with known secret keys, the attacker can manage to eliminate the parity of values stored in DFFs and then analyze the parity of SFFs, which reveals the secret key of the attacked circuit.

Fig. 2.9.a shows a slice of the DfT structure with SFFs and DFFs. SFFs are part of the intermediate register while DFFs are related to the input through an unknown (to the attacker) function FU. Given the input pair (Mj, Mk), the attacker can measure the test output H difference ($Diff_{j,k}$). Output H has two components: the parity of SFFs (HS) and parity of DFFs (HD), as shown in Fig. 2.9.b. A priori the attacker does not know either of these components. For the input pair (Mj, Mk), a difference on HS is called $SDiff_{j,k}$ and a difference on HD is called $DDiff_{j,k}$.

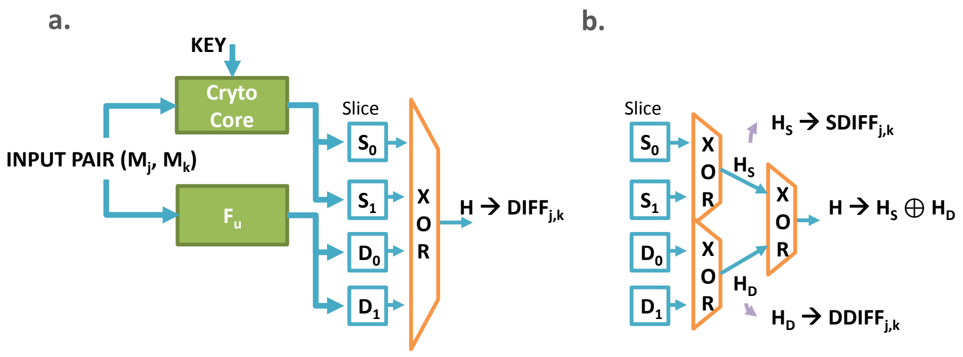


Fig. 2.9: (a) Example of slice with SFFs and DFFs with unknown function; (b) Equivalent DfT structure

In order to retrieve the HS component (then measure the signature dependent only on SFFs) the attacker must have access to two other identical circuits for which he or she knows the secret keys. The circuits being identical, the DfT is also identical. Then circuits A and B have distinct secret keys KEY_A and KEY_B. The attacked circuit is called C and its secret key is KEY_C. The attack is divided into two steps. First the attacker uses A and B to find out the component HD for a sequence of input pairs, then applies the same sequence of input pairs to circuit C, to finally measure the signature at H and remove the component HD. Afterwards, the result obtained is a measured signature HS dependent on the KEY_C.

First, the attacker applies the sequence of input pairs that generates unique signatures to both circuits A and B. Afterwards, he or she measures the differences at the output H. The measured signature for a circuit X, called $MSIG_X$, is a concatenation of the output differences for each input pair:

$$MSIG_X = Diff_{0,1}^X \,||\, Diff_{2,3}^X \,||\, Diff_{4,5}^X \,||\, Diff_{6,7}^X \,||\ldots \quad (16)$$

The measured signatures for circuits A, B and C can be written as Eq. 17-19:

$$MSIG_A = SDiff_{0,1}^A \oplus DDiff_{0,1} \,||\, SDiff_{2,3}^A \oplus DDiff_{2,3} \,||\, SDiff_{4,5}^A \oplus DDiff_{4,5} \,||\ldots \quad (17)$$
$$MSIG_B = SDiff_{0,1}^B \oplus DDiff_{0,1} \,||\, SDiff_{2,3}^B \oplus DDiff_{2,3} \,||\, SDiff_{4,5}^B \oplus DDiff_{4,5} \,||\ldots \quad (18)$$
$$MSIG_C = SDiff_{0,1}^C \oplus DDiff_{0,1} \,||\, SDiff_{2,3}^C \oplus DDiff_{2,3} \,||\, SDiff_{4,5}^C \oplus DDiff_{4,5} \,||\ldots \quad (19)$$

The terms $DDiff_{j,k}$ are the same for the three measured signatures because the component HD is independent from the secret key. Next, the attacker calculates the difference between the measured signatures $MSIG_A$ and $MSIG_B$:

$$MSIG_A \oplus MSIG_B = SDiff_{0,1}{}^A \oplus SDiff_{0,1}{}^B || SDiff_{2,3}{}^A \oplus SDiff_{2,3}{}^B \ldots \tag{20}$$

All $DDiff_{j,k}$ terms are eliminated in Eq. 20, leading to values depending only on $SDiff_{j,k}$ terms, since $DDiff_{j,k}$ terms never change in the 3 measured signatures. The secret keys KEY_A and KEY_B are known, but the attacker does not know which SFFs subsets belong in the attacked slice. This information must be known to derive the KEY_C. For each subset of observable SFFs there is only one simulated signature table. If Ns is the number of SFFs in the intermediate register, there are 2^{Ns} possible subsets of observable SFFs, and thus 2^{Ns} signature tables. Each signature table has different signatures for KEY_A and KEY_B (uniqueness property). One of these signature tables must contain the signatures for KEY_A and KEY_B, which are expressed in $SDiff_{j,k}$ terms (the simulation considers only SFFs). In order to find out which table contains the right signatures, the attacker calculates the difference of signatures for the KEY_A and KEY_B for each table. The signature table with a match corresponds to the SFFs subset compacted in the attacked slice. Additionally, this signature table contains the signature for circuits A and B (with $SDiff_{j,k}$ terms only):

$$SIG_A = SDiff_{0,1}{}^A \; || \; SDiff_{2,3}{}^A \; || \; SDiff_{4,5}{}^A \; || \ldots \tag{21}$$
$$SIG_B = SDiff_{0,1}{}^B \; || \; SDiff_{2,3}{}^B \; || \; SDiff_{4,5}{}^B \; || \ldots \tag{22}$$

In order to find the component HD of the signature the attacker computes the difference between SIG_A and $MSIG_A$, eliminating the $SDiff_{j,k}$ terms:

$$DDiff_{0,1} \; || \; DDiff_{2,3} \; || \; DDiff_{4,5} \; || \ldots \tag{23}$$

The final step consists in adding Eq. 23 to the measured signature of circuit C (Eq. 19) to obtain a signature of C free of DFF-dependent terms. The attacker proceeds by searching in the simulation table that corresponds to the subset of SFFs (obtained early in this section) the signature matching the signature of C. The matching line corresponds to the right key (KEY_C).

Conclusions

With this work we presented a new scan-based attack. It is generic and can be easily adapted to different classes of symmetric and asymmetric ciphers such as AES, DES, Khazad, ECC, RSA and ElGamal. It works against advanced DfT structures such as response compaction, mask decoders and time compaction. Additionally it does not require advanced knowledge of the circuit or test structure details. It has been applied to various gate-level netlists in order to validate the approach.

The results of these works have been published in the papers [J12], [J13], [S22], [S23], [S25], [S27], [W15] referenced in the Publication list.

3.6.2. Countermeasures against Scan Attacks

This subsection presents 4 countermeasures that we proposed in the last 5 years. The first basic (and trivial) countermeasure against scan attacks is based on not using scan chains. A Built-In Self-Test approach is used instead. The second proposed countermeasure is based on the internal comparison of actual test responses and expected ones (that must be provided by the external tester). The comparison is performed vector-wise not to allow scan attacks. The third countermeasure is a smart and small test controller that does not impact the test procedure, while guaranteeing the security against the scan attacks. The last approach is an authentication method embedded in the JTAG standard to allow authentication of both the circuit to the tester and from the tester to the circuit.

Built-In Self Test

One approach for providing test solutions at different stages of an IC life cycle consists in including Built-In Self-Test (BIST) resources into the Circuit Under Test (CUT). Classically, storage elements are organized into scan chains and additional hardware is used for feeding the scan chains with pseudorandom test data, and sinking the test responses before analysis of the compressed signature. So, BIST does not provide full controllability and observability of the internal storage elements from the IC interface. This major difference with the external testing strategy makes the scan- based attacks not exploitable. However, BIST must be implemented at low cost and its efficiency must be demonstrated in terms of fault coverage and test length.

Security provided by block cipher algorithms such as DES and AES relies on two main properties named Diffusion and confusion. Confusion refers to making the relationship between the key and the ciphertext as complex and involved as possible. Diffusion refers to the property that redundancy in the statistics of the plaintext is dissipated in the statistics of the ciphertext. For diffusion to occur, a change in a single bit of the plaintext should result in changing the value of many ciphertext bits. These properties are supported by the Feistel network for the DES and by the substitution–permutation network for the AES. AES and DES also have two common characteristics. First, they are iterative algorithms. DES is composed of 16 rounds while AES is made of 10 rounds. All rounds are (quasi) identical, i.e., the result of a round is used as the input of the next round. Second, since encryption/decryption are bijective operations for a given key, each round is a bijective operation too (on a set of 2^{64} elements for DES on a set of 2^{128} elements for AES).

The diffusion property is a very interesting feature with regard to the test of their hardware implementation. It implies that every input bit of a round influences many output bits, i.e., every input line of a round is in the logic cone of many output bits. In other words, an error caused by a fault in the body of the round is very likely to propagate to the output. Thus, the circuit is very observable. Moreover, since rounds are bijective, the input logic cone of every output contains many inputs. In other words, each fault is highly controllable. Therefore, these circuits are highly testable by nature whatever the implementations.

Fig. 2.10 presents a typical implementation of the AES or DES crypto-algorithm. It is mainly composed of a Key Generation module and a Round module. In mission mode, after an initial operation (XOR between Key and Plaintext for AES, and permutation of the plaintext for DES), the plaintext block is looped around the Round module several times (10 for AES, 16 for DES) before the final cipher is loaded into the R-out register, possibly after a final operation like the final permutation in DES. The widths of the data are 128 for AES and 64 for DES.

The idea of the BIST architecture is to use the circuit as it is, by slightly modifying the Control unit so that the circuit performs more than the nominal rounds. In other words, we expected that thanks to the intrinsic easiness of being tested, by letting run the circuit for several clock cycles, the final fault coverage will be high enough. We have conducted a theoretical study that allows calculating in advance the number of encryptions needed to reach 100% fault coverage with a given confidence level. The theoretical number of required encryptions for 100% fault coverage is then confirmed by fault simulation.

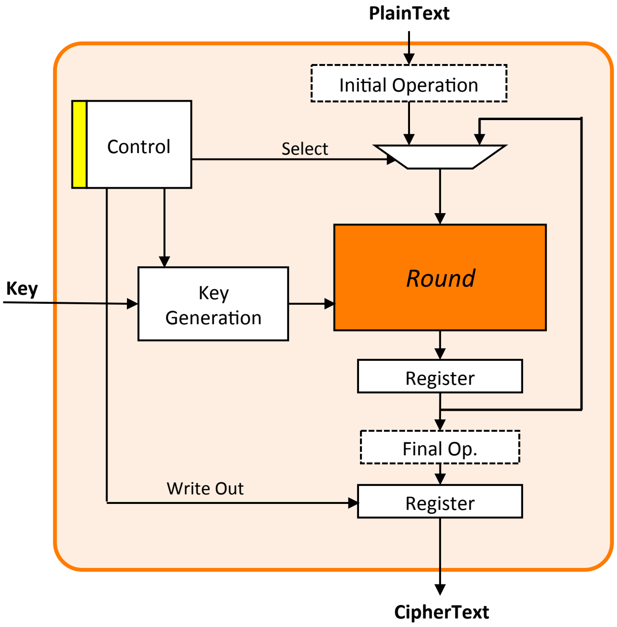


Fig. 2.10: Implementation of the crypto-algorithm

We considered the following aspects:

1. The stream generated by a crypto-algorithm when the input is fed by its output can be considered as random.
2. The presence of a fault modifies the round output and thus the next test pattern (circular scheme). This is taken into account in our experiments in which we injected every single stuck-at fault, fault simulated the circuit, and only observed the value of the final signature produced by the crypto-core (DES or AES).
3. One of the operations of the crypto-algorithm is a substitution function that is implemented by S-boxes. S-boxes represent the largest part of the crypto-cores. Their inputs are independently fed by a subpart of the round inputs. We can therefore assume that they are fed by a random source, receiving a pattern every clock cycle.
4. An S-box needs k deterministic patterns to be fully tested and it receives one random pattern every clock cycle.
5. Other parts of the round module (mainly wires and XOR operations) receive one pattern every clock cycle as well. Since the other parts have lower complexity than the S-boxes, it can be expected that they will be fully tested by the time the S-boxes received a sufficient number of test patterns.

The theoretical number of required clock cycles (or patterns) can be precomputed as the theoretical number of clock cycles for testing the S-boxes. The following equation gives the length (n) of the minimal-length random sequence that includes the k targeted test patterns with a given confidence level P, with p being the probability of each pattern to appear:

$$P[X \leq n] = 1 - \sum_{i=1}^{k} (-1)^{i+1} \binom{k}{i} (1 - ip)^{n}$$

We applied the equation to both the DES and the AES.

For the DES algorithm, we considered a confidence level of P=99% for a sequence of k=64 patterns. This sequence represents an upper bound since it corresponds to the exhaustive test set for any six-input S-box. Each pattern has the same probability to appear in the pseudorandom scheme, i.e., p=1/64. From the equation, it comes that the minimal-length random sequence is n=540 patterns. According to the implementation of the S-boxes and the actual number of required test patterns k (that is usually smaller than 64), the length of the test procedure can vary from 440 clock cycles (28 encryptions) to 540 cycles (34 encryptions). Experimental results confirmed our hypothesis. We fault simulated the DES with several keys and initial input messages. After 25 encryptions (i.e., 400 clock cycles), the whole circuit (round module and control module) has always been fully tested.

For the AES algorithm, it comes that the minimal random sequence length should include n=2593 random patterns for exhaustively testing the AES S-boxes (k=256) with a confidence level of 99%. For various implementations of the AES S-boxes and thus for different deterministic test sets, we calculated the length of the random sequence for including the k targeted deterministic patterns. The minimal length is ranging from 2400 to 2593 patterns depending on the implementation. This hypothesis has been confirmed during the experiments since 100% fault coverage has been achieved on the whole circuit (round module, key generation module, controller) after 210 encryptions (i.e., 2100 rounds). This experiment has been repeated with different plaintexts and secret keys as starting points, and we obtained test sequences ranging from 2100 to 2500 patterns.

To conclude, BIST approaches are effective for secure circuits since they have the intrinsic property of being easily controllable and observable. Since BIST does not rely on visible scan chains, it is a natural countermeasure against scan-based attacks. Conversely to standard BIST solutions, the technique we proposed entails a negligible area overhead. The principle of the self-test procedure is to feed the core with its own output and let the device run for a certain number of encryptions, and then to compare the output of the final encryption with a precomputed signature. In a very short test time, 100% of fault coverage is achieved. Nevertheless, BIST approaches do not allow diagnosis of faults, nor debug of possible problems.

The results of this work have been published in the paper [J9] referenced in the Publication list.

Internal Comparison

A common industrial practice to avoid scan-based attacks is to physically disconnect the scan chains after production testing by blowing fuses located at both ends of the scan chains. However, this solution impedes the testing of those devices requiring being tested after manufacturing. In particular, the correct behavior of the secure circuits should be validated after the introduction of the secret key, which can be programmed at any time of the circuit's lifecycle. This secured information can indeed be owned by any circuit producer (e.g. designer, manufacturer, system integrator) or user (e.g., reseller or final customer). In addition, scan disconnection stops any further analysis, e.g. diagnostic, or cannot be considered as an appropriate response to the scan attack if the connection can be reconstructed.

In the standard scan-based test mechanism, FFs are replaced by Scan Flip-Flops (SFF) and are connected so that they behave as a shift register in test mode. The output of one SFF is connected to the input of next SFF. The input of the first FF in the chain is directly connected to an input pin (Scan-In) while the output of the last FF is directly connected to an output pin (Scan-Out). An additional signal (Scan-Enable) selects whether SFFs have to behave normally or as a shift register. The test procedure is composed of 3 steps: first, test patterns are shifted-in via the scan chain (i.e., by keeping Scan-Enable=1) for #SFF clock cycles (where #SFF is the number of SFFs in the chain). Second, one or two functional clocks (i.e., Scan-Enable=0) are applied to capture the circuit's response. Usually, one clock cycle is used for static faults, while 2 (or even more) clock cycles are used for dynamic faults. Finally, the content of SFFs is shifted out for #SFF clock (again, with Scan-Enable=1) to allow the ATE to compare the obtained values with respect to the expected ones.

The principle of the approach we proposed is to compare the actual responses with the expected ones within the chip boundaries instead of scanning-out the actual responses and comparing it within the ATE. In order to guarantee that secure data cannot leak outside the chip, the output of the comparison is not bitwise delivered to the ATE, but only after applying and comparing the whole test vector (i.e., after comparing the value of each SFF). Therefore, a potential attacker can no longer observe the FFs content but simply pass/fail information for the whole test vector.

The general scheme of the proposed Secure Comparator is shown in Fig.2.11. Instead of directly shifting DUT's responses (`Sout`) out of the chip, the ATE also provides the expected responses using the `Sexp` pin and the actual test response is on-chip compared with the expected one. After having compared all #SFF bits captured in the scan-chain, the signal `TestRes` is asserted if the whole test vector matches the one with expected values.

The Secure Comparator is composed of 3 parts: the *Sticky Comparator* responsible for the comparison between the bit stream coming from the scan chains and the expected values, and the *Output Enabler* triggering the final comparison result. Finally, the *I/O Buffers* allow keeping the test pin count as in a classic scan-based approach.

The *Sticky Comparator* performs a bitwise serial comparison between the bitstream coming from `Sout` and the one from `Sexp`. A FF (Flag in the figure) is initially reset and then it rises to '1' whenever one comparison fails. The reset of the flag is performed when the scan operation is not enabled (i.e., `Sen`='0'). This means then when the circuit goes from capture to test mode, the flag becomes meaningful and its value designates whether the two bitstream are equal or not.

The *Output Enabler* permits the observation of the `TestRes` only after comparing the whole test vector. It is composed of a down counter with parallel load that loads the value #SFF whenever the scan operation is not enabled. Therefore, when the circuit goes to test mode, it start counting and after #SFF clock cycles its terminal count allows outputting the `TestRes` signal through the AND gate.

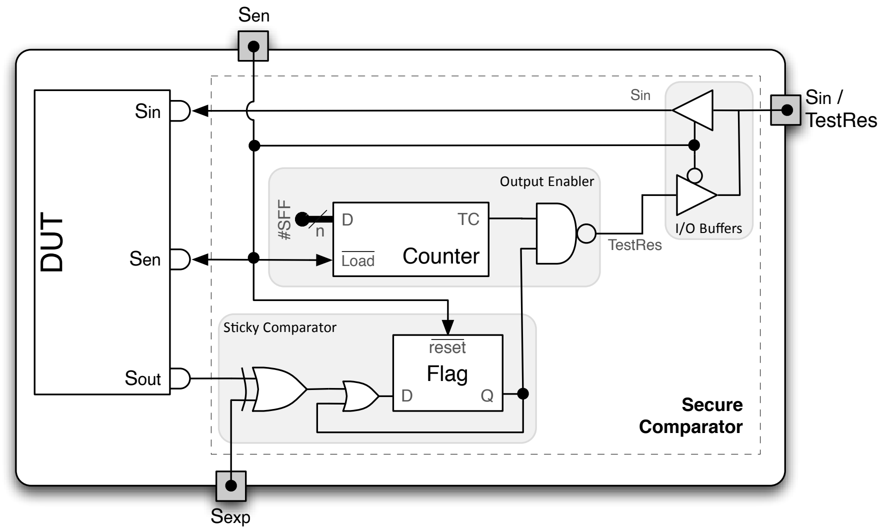


Fig. 2.11: Secure Comparator

The *I/O Buffers* allow sharing the same pin for `Sin` and `TestRes`. A classical scan based design requires 3 signals: scan-in, scan-out and scan-enable. The proposed solution requires, besides `Sin` and `Sen`, the `Sexp` signal (that replaces Sout) and the additional `TestRes`. However, `Sin` and `TestRes` are not used at the same time, therefore it is possible to use bi-directional buffers shared between them, as shown in Fig.2.11. During the shift operation the pin can be set as input and used by the tester to feed the circuit with the input vectors, whereas during the capture operation the pin is activated as output to deliver the previous comparison result.

Concerning the area cost, on-chip comparison is necessary for sensitive scan chains only (the others can be treated in the usual way). However, while the *Sticky Comparator* is required for every scan chain, all sensitive chains can share the same counter of the *Output Enabler*. For a circuit with S scan chains, the longest one being composed of #SFFs, this Secure Comparator requires:

- S flip flops and 2 · S logic gates (XOR+OR) for the Sticky Comparator;
- 1 counter able to count from Log2(#SFFs) to 0, and S NAND gates to filter the TestRes signals;
- 2 · S buffers.

For example, a circuit with 32 scan chains of 10000 SFFs each, have an extra cost of 32 FFs, 98 combinational gates, 64 buffers and one 14-bits counter. This overhead represents a negligible cost compared to the size of a circuit.

Concerning the security of the proposed scheme, the role of the proposed Secure Comparator is to avoid the observation of SFFs containing secret information. If the result of the comparison was accessible at each clock cycle instead of each test vector, an attacker could easily observe the scan chain content by shifting in "000…000" on the `Sexp` pin. Each bit-comparison would then validate that either the actual bit was '0' when `TestRes`=1 and vice-versa. On the contrary, with the proposed vector-wise comparison the only way to retrieve the sensitive data information is to apply a brute-force attack by trying every possible response until `TestRes` is asserted. This attack would thus require $2^{\#SFF}$ attempts.

Concerning the testability of the circuit, The *Secure Comparator* does not impact the fault coverage. In fact, each test response is compared to the expected one as in a classical ATE-based test scheme. Therefore, the achievable fault coverage is not altered. Test time is not increased either, since the expected responses are scanned-in at the same time as the next input vector is scanned-in. A limitation of our technique is related to the presence of possible unpredictable values in the SFFs. Computing expected values for on-chip comparison is indeed no longer possible. To fix this limitation, the *Sticky Comparator* should ignore the comparison result (and keep unchanged its flag) when `Sout` is unknown. This can be implemented by providing an additional mask signal that is asserted when needed. However, an attacker must not be able to mask as many bits as wanted. In fact, if it were possible to mask all but one bit, it would be obvious to discover the value of each single bit in the scan response. This would reduce the complexity of the brute-force attack from exponential ($O(2^{\#SFF})$) to linear (O(#SFF)). Therefore, the number of masked bit (per test vector) must be limited to P such that a brute force attack on $2^{\#SFF-P}$ remains unfeasible. The extra cost to tolerate unknown values includes an extra pin for the mask, a $\log_2 P$ counter to limit the number of masked bits and 2 logic gates. Fig. 2.12 shows a possible implementation.

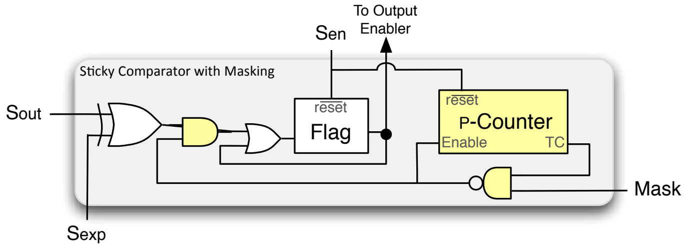


Fig. 2.12: Sticky Comparator with Masking

Limited observation of the scan chain content raises the question of whether fault diagnosis is affected. In a classical test scheme, the content of the whole scan chain after application of a test vector is shifted-out to the ATE and analyzed to identify possible locations of the fault. In the proposed scheme, since only pass/fail information is shifted-out, it is not possible to differentiate which faults cause a wrong response. However, in order to discriminate these cases, it is actually possible to enter, for every test vector, the whole set of possible wrong expected responses that have been pre-calculated by resorting to the fault dictionary. Therefore, the proposed Secure Comparator allows the same diagnostic resolution as it can be obtained with the classical scan scheme. The only difference resides in the matching procedure between the obtained responses and those stored in the fault dictionary. In the classic scheme this is done off-line (i.e., after collecting all responses from the circuit), while in our case all faulty responses must uploaded on the DUT thus requiring additional time. Problems still exist in the case of debug. Indeed, in this case, the fault response is not known in advance, thus limiting the proposed approach.

The results of these works have been published in the papers [J16], [S26], [P25] referenced in the Publication list.

Smart Test Controller

We have recently proposed a smart test controller that exploits the following observations:

- The scan-based test of digital circuits follows a predefined scheme: input vectors are shifted-in via the scan-in (with scan-en asserted), one functional clock cycle is applied (also known as capture cycle, with scan-en not asserted), and output responses are shifted-out via scan-out (while, at the same time, the next input vector is shifted in). When delay faults are targeted and the Launch-On-Capture technique is used, 2 capture cycles may be required.
- Known attacks are based on the fact that the circuit is first run in normal mode for a certain number of clock cycles in order to bring the circuit to a desired state (for instance in the AES, the circuit is run up to the first encryption round). Then the scan chain is used to observe the state of the circuit in that moment.

The principle of the proposed controller relies on the masking of the scan-out signal in such a way that it does not deliver any sensitive data until the whole scan chain is first freshen. Fig. 2.13 sketches the Circuit Under Test (CUT) connected to the proposed smart test controller, while Fig. 2.13 details its finite state machine. The controller reads the scan-en signal and, based on its value, it forces to 0 the OUT_en signal that drives a 2-bit AND gate whose other input is the CUT's scan-out.

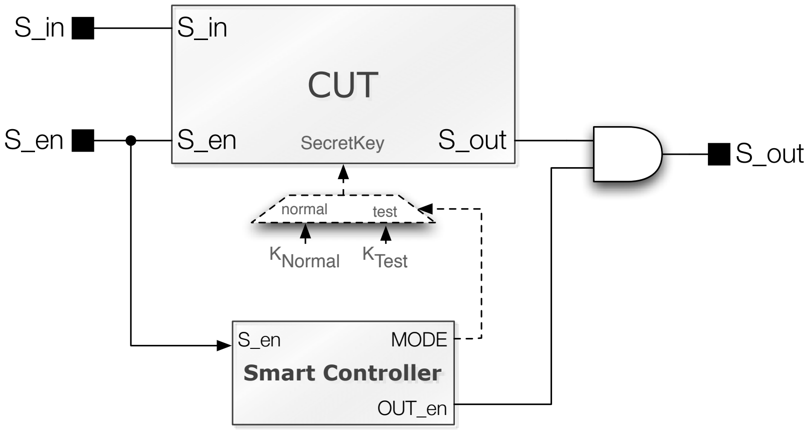


Fig. 2.13: The Smart Controller within the original design

The controller is automatically armed at power-on (Normal state). Once it is armed, OUT_en is forced to 0 in order to filter any shift-out operations. In this initial state, a down-counter is set to #L, i.e., the number of scan flip-flops in CUT. After #L consecutive clock cycles with scan-en asserted (Flushing state), the controller is disarmed. During the Flushing state, the controller is still armed (OUT_en=0) to prevent the observation of the scan chain content after a normal execution (i.e. scan attacks). After disarming the controller, OUT_en is set to 1 so that any scan operation is performed without masking. The controller allows one or two capture cycles (Stuck-At-Capture and Delay-Capture states) without re-arming OUT_en. If more than 2 capture cycles are executed, the controller goes back to the Normal state. The Shifting state allows shifting input vectors into the scan chain. The down-counter is not used in this state because the sensible data already disappeared from the scan chains. In this way, the controller enables the test of the scan-chain itself where longer than #L sequences are shifted without capture cycles.

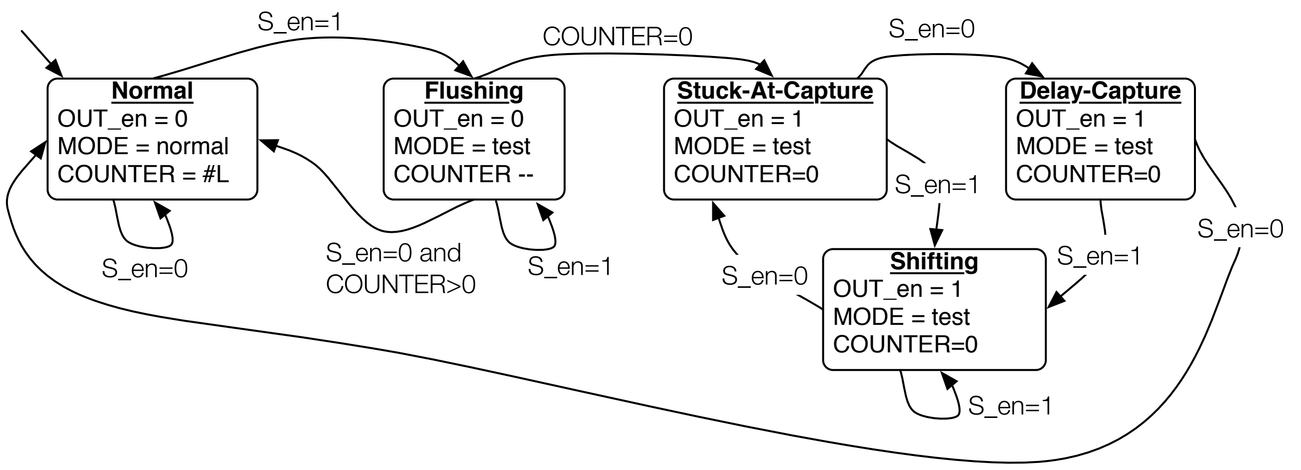


Fig. 2.14: Finite State Machine of the Smart Controller

The controller allows identifying two execution modes: normal and test (MODE signal). Nevertheless, it does not require any additional signal to force one of the two modes since the detection of the mode is performed automatically: the Normal state is the normal mode, while all the other states define the test mode. the controller automatically detects. The execution mode may be possibly used when two secret keys are used (as shown with dotted lines in Fig. 2.13).

The security of secure devices using the proposed controlled is guaranteed by the fact that it is not possible to bring the circuit in a desired state and then to shift out the content of the scan flip-flops. Indeed, the first time the scan chain is shifted out, the scan-out signal is forced to 0 for #L clock cycles. After this phase, the circuit can be fully tested. However, as soon as the attacker tried to run more than 2 functional clock cycles (to possibly reach the desired state), the controller would be armed again and the next scan-out operation would be masked.

This controller can be inserted into the design at the very end of the design, thus not perturbing the overall design flow. It is also transparent to the tester because it does not modify the classical and standard test procedures. The area introduced by the controller is meaningless.

The results of this work have been published in the paper [S29] referenced in the Publication list.

Authentication-based Test Controller

This work has been carried out within a cooperation between the LIRMM and the Catholic University of Leuven. We sought to provide security features to the IEEE 1149.1 JTAG interface by including a Schnorr-based secure test protocol, and to provide an efficient hardware implementation of the protocol using elliptic curve cryptography. This is the first work that proposes a mechanism for mutual authentication between the secure device and the tester based on a well known and studied public key authentication protocol.

In this work, we solve the inherent key-management problem of existing Symmetric-Key Cryptography (SKC) based secure JTAG approaches using Public-Key Cryptography (PKC). Specifically, if SKC is used for securing JTAG, there will be a common master secret key for all products or a large secret-key database needs to be maintained at the tester/updater side, which are not good options for mass electronic products. PKC implementations are inherently more hardware expensive and slower than SKC based approaches. Therefore it is a challenging task to incorporate PKC in a resource constrained environment like JTAG.

The use of asymmetric primitives and the related public/private key pairs substantially improve the complexity involved in key management in this setting of tester against the device. If we take for example the automobile industry, then we expect to bring our car to virtually any garage in the world and get our car serviced. Servicing cars now also includes updating software in one of the on-board units (OBUs) which may be through the JTAG interface. Currently these updates can be pushed to the OBU as soon as it is powered on; no other security measures are used. One of most important reasons for the current lack of authentication is the fact that it presents car manufacturers with a large key management problem that is inherent to the use of symmetric solutions in large scale systems. In symmetric solutions, the verifier needs a copy of the same key that was also used to generate the authentication token (e.g., a message authentication code or MAC on the firmware). This implies that the use of a single master key is very risky as it will be wide spread in many devices and likely to leak at one point in time. Therefore, symmetric key based solutions require unique keys to be installed at every verifier. In large scale systems, this would require a large database that link the identity of the prover to its key and a means for verifiers to securely access and authenticate this service. Alternatively, key derivation schemes could be used, but they only lower the risk related to a single master key.

To overcome this problem, the solution proposed in this work offers the possibility of using certificates instead of shared symmetric keys. This would for example allow the use of the same signed firmware update for a wide range of OBUs, without the risk of installing the same symmetric key in this range of devices. They just need a valid copy of the manufacturers' public key for signature verification.

We use an enhanced version of ECC-based Schnorr Protocol as the public-key cryptographic protocol in our secure JTAG test scheme. Various public-key implementations, such as RSA or ECC, may be used to solve the key-management problems present in previous secure JTAG approaches. We chose ECC as it offers the same security as RSA, with much smaller area footprint. Area overhead is of critical importance, since we are constrained in terms of silicon area required to incorporate security features into JTAG, owing to the small test interface available in most applications. Similarly, various protocols using ECC may been used. We chose the Schnorr protocol as it is provably secure and allows efficient implementation on space-constrained hardware.

An added positive side-effect of Schnorr is that it is “zero- knowledge” and thus no information about the secret key of the prover leaks during a protocol run. The zero-knowledge property may be useful in an uncontrolled in-the-field code update, debug or test environment where the communication channel between the test server and JTAG is untrusted and the secret need not be shared or linked to a communicating entity.

Our proposed architecture is shown in Fig. 2.15. The ordinary JTAG circuitry is enclosed within dotted lines, and it is divided into its two main components: the TAP finite state machine and the instruction decoder. The Schnorr protocol is performed by the Schnorr controller, placed in the center of Fig. 2.15. It interacts with a modified JTAG instruction decoder, ECC module, and a 192-bit random number generator (a Linear Feedback Shift Register). The base point coordinates (curve parameters) are fetched from an external non-volatile memory. The system is supposed to be locked in the beginning. In order to unlock it, the tester must manipulate the JTAG inputs to enter the new ‘UNLOCK’ instruction. Then, the instruction decoder informs the Schnorr controller to start the protocol, by means of the ‘request_unlock’ signal. As soon as the authenticity of the test server is verified, the Schnorr controller activates the ‘release_unlock’ signal, informing the instruction decoder that other instructions can now be performed. For instance, if the system is unlocked, the design under test (DUT) boundary scan register can be controlled. Meanwhile, when ‘release_unlock’ signal is not active, the instruction decoder sets the multiplexer ‘MUX1’ to always select the output from the multiplexer ‘MUX2’, which is controlled by the Schnorr controller, impeding the shift out of any DUT specific register.

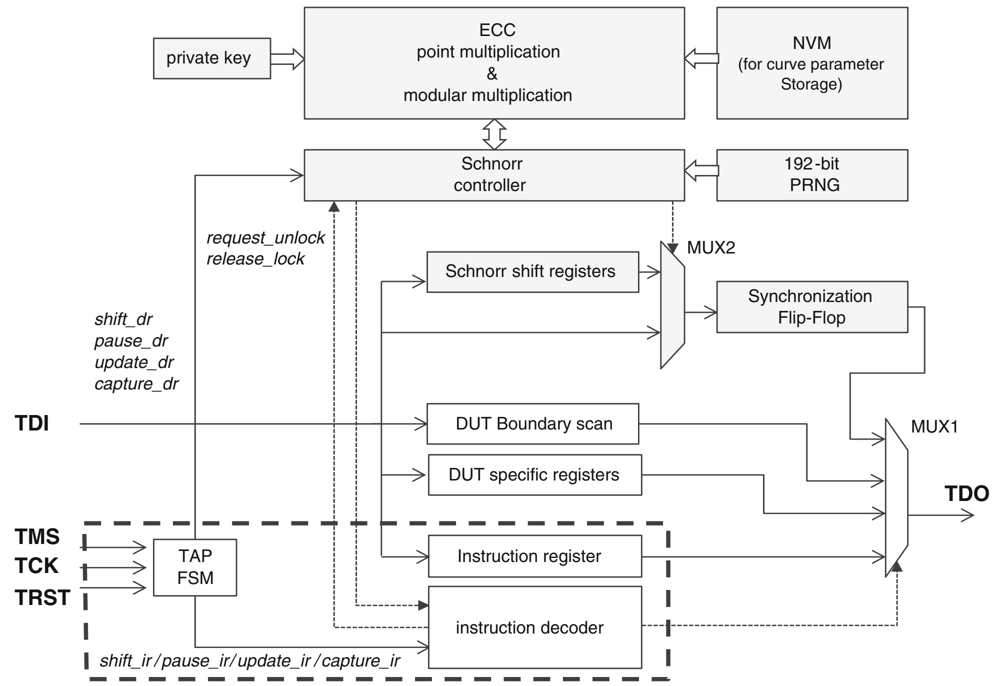


Fig. 2.15: JTAG-ECC Controller

During the protocol execution, the communication with test server consists of using the Schnorr shift registers (192 bits) to shift in and out information required for the protocol. It is important to notice that the shifting is always controlled by the test server, and that the timing for executing point multiplications depends on the scalar multiplier. It means that the Schnorr controller must inform the test server that it has finished each operation of the protocol. This synchronization is achieved by always adding one flip-flop at the end of the Schnorr shift register that is set to'1' if the information in the shift register is valid, otherwise the multiplexer 'MUX2' selects the TDI input and the synchronization flip-flop is set to '0'. Thus, the test server keeps on shifting at least this one bit to detect that the Schnorr controller is ready for receiving the next data.

We made a detailed hardware implementations, area and timing results for our ECC-based authentication protocol, by showing that the whole circuit can be synthesized in less than 25K gates.

The results of this work have been published in the paper [J15] referenced in the Publication list.

3.7. Fault Attacks

Fault-based attacks rely on perturbation of the circuit and use (expected) production of erroneous results for inferring secret information. Formally, the faults reflect the physical conditions that cause a circuit to fail to perform in a required manner. The error is the visible aspect of the fault, i.e. a wrong observable signal produced by the defective device. The fault set induced by fault-based attacks includes transient faults on combinational gates, and bit-flips on memory elements.

Several techniques can be used for fault injection. They rely either on perturbation of the environmental conditions (e.g. power supply, clock), or, for higher cost and better precision, on injection of transients or bit-flips on target signals (e.g. faults injected through laser beams).

There are two forms of countermeasures against fault-based attacks: sensor-based and error-detection-based countermeasures. The former ones aim at detecting inappropriate environmental conditions (for instance, unexpected light, clock glitches, or additional current in the substrate of the CMOS device). The second is based on the use of information redundancy to detect the presence of errors.

In the last 5 years we actively worked on the proposition of new error detection methods for fault attacks, both sensor-based (by integrating built-in current sensors) and error-detection-based. Moreover, we have developed a fault simulator tool that is able to simulate the effect of a laser injection in a CMOS device and to perform the simulation of the whole circuit. The simulation has been used to validate the effectiveness of the proposed countermeasures. The next subsections will describe the sensor-based countermeasure, the error-detection-based countermeasures, and finally some highlight on the fault simulator.

3.7.1. Sensor-based Countermeasure

Built-in current sensors (BICS) were initially proposed as a mechanism for detecting large increases in the current IDDQ consumed by a CMOS circuit during its quiescent state, i.e. when the circuit is not switching. Further, BICS were also adapted for detecting transient faults in memory cells. Recently, efforts were made for monitoring transient faults in combinational logic as well for security purposes. The principle of a BICS is to monitor the current between the power lines (VDD and GND) in order to distinguish anomalous transient currents from normal currents. The today's problem is that the amplitude of transient currents induced by radiation effects or fault attacks can have the same order of currents normally generated by switching activities in combinational logic circuits. Hence, schemes monitoring power lines are very limited for detecting just small range of transient faults.

On the other hand, BICS connected to the bulks of the monitored circuit's transistors are able to detect a wider range of transient faults. We have proposed a Bulk-BICS (BBICS) circuit that allows detecting the presence of suspicious current in the bulk of the circuit. Moreover, since this circuit increases the overall power consumption, we have introduced a sleep-mode. Fig. 2.16 sketches the architecture of the proposed BBICS. The BBICS is designed for monitoring NMOS bulks in pull-down networks (BBICS for PMOS transistors is not described here). Wmin represents the minimum diffusion width of the transistors of a 32-nm CMOS technology, Lmin is the minimum channel length, and the design factors X and Y are used for calibrating the sensors, as discussed later.

The BBICS is mainly composed of a latch (transistors 5, 6, 7, and 8) that are responsible for amplifying the anomalous transient currents coming from the bulk "NMOS_Bulk" of the monitored block. Higher gain of amplification is obtained by increasing X and Y, hence higher BBICS's sensitivity in detecting transient faults is also determined in terms of these design factors. BBICS's latch has, moreover, the function of memorizing a flag in case of a transient fault within a defined current range. On the other hand, as soon as the flag of fault is processed by higher instances of the system, BBICS's latch must be reset (through the input "Reset") in order to detect other transient faults.

By growing the factor X, transistors 6 and 8 allow improving the BBICS's sensitivity in detecting transient faults. However, it also contributes considerably to the increase of static power consumption, which is today responsible for up to 50% of the power dissipation of systems based on ultra-deep submicron technologies. In fact, if higher BBICS's sensitivity is the goal, greater X and amplification have to be designed to increase the diffusion widths of transistors 6 and 8, and then decreasing their v_{th}. These lower v_{th} make thus possible to switch "Flag_N" (from GND to VDD level) with lower amplitudes of anomalous transient currents (i.e. transient faults of smaller charges that flow from "NMOS_bulk" through transistor 2 up to node "Flag_N").

To reduce static power consumption we introduced transistor 9 that allows the utilization of a sleep-mode when the system is left on standby. Transistor 9 is, in this case, set "on", making a less resistive path between the node "NMOS_bulk" and GND. Consequently, Vgs of transistors 6 and 8 approach to zero, Isub becomes much lower, and thus the static power consumption is drastically reduced.

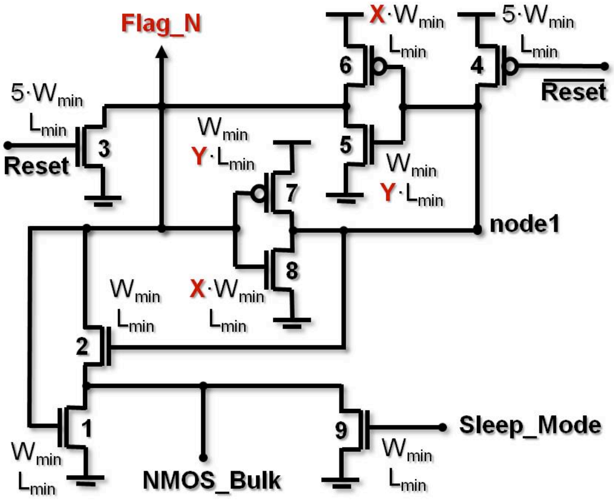


Fig. 2.16: The proposed NMOS sleep-mode improved BBICS

Transistor-level simulations allowed comparing our Sleep-mode Improved BBICS with state-of.the-art solutions, showing its effectiveness in terms of both detectability of transient current pulses and low power consumption.

This work is now part of a collaborative project between the LIRMM, the ENMSE (Gardanne) and the TIMA lab. The goal is to actually produce a CMOS circuit implementing this sensor.

The results of this work have been published in the papers [J14], [J11], [P33], [W18], [S28], [P24], [S24], [C11] referenced in the Publication list.

3.7.2. Error-detection-based countermeasures

Error detection codes consist in checking for possible mismatch between a code predicted for an output from the current input, and the code of the actual output of the process. Code prediction is performed in parallel with the main process (algorithm, round, operation) in such a way that predicted and actual codes can be compared at the end.

In one of our first works, we proposed a solution that focuses on S-boxes of the AES. The principle is to add two parity bits per S-box, one parity bit for the input byte and one for the output byte, and therefore the logic for predicting such information (see Figure 2.17). The actual output parity is compared with the predicted output parity bit, and the actual input parity bit is compared to the predicted one. When the S-box and the prediction circuits are synthesized as combinational logic, the area overhead is 38.33% with respect to the original S-box. This solution allows detecting an additional 27% of errors of even multiplicity, besides all odd multiplicity of errors. By combining the double parity with solutions that allow protecting the whole AES round, we proposed a couple of architectures that are described in [B2].

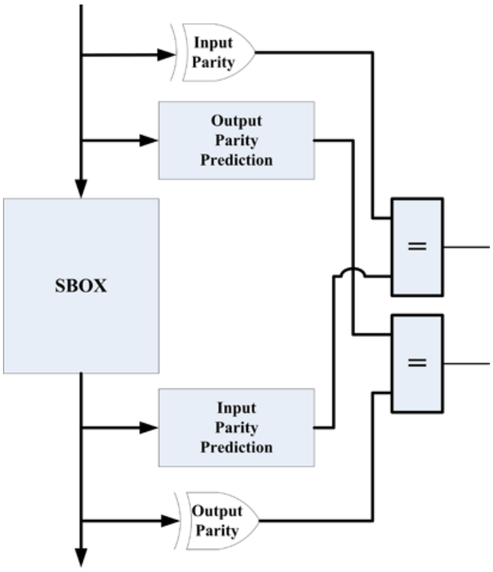


Fig. 2.17: Double Parity bit for the Sbox

We also carried out a major contribution in the domain by deeply analyzing the effect of the fault in the circuit and the strength of the detection code. Indeed, a detection code may be very strong to detect a particular set of error, while the fault induced by the attack generates a totally different error. We conducted extensive experiments in order to show the error profiles resulting from the injection of a single transient bit-flip fault (representative of faults injected by means of a laser beam), and the real effect (i.e., the error) at the output monitored by the detection mechanism. This information can be used for choosing the appropriate code-based detection scheme. This study showed how a different design and synthesis style can have big impacts on the behavior of the circuit under attack. [B1] and [B2] report the detailed results.

The results of this work have been published in the papers [B1], [B2], [S21], [S20], [W10] referenced in the Publication list.

3.7.3. Fault Simulator

In order to validate countermeasures against fault attacks, we developed a fault simulator that we called LIFTING (LIRMM Fault Simulator). It allows performing 0-delay and delay-annotated fault simulation for single/multiple stuck-at faults, Single/ multiple Event Upset (SEU) and single/multiple event transient (SET) on digital circuits described in Verilog. Moreover, it allows integrating faults that are described at spice level, by performing multi-level simulations. LIFTING is an open-source project.

The proposed tool is implemented to operate on a set of tables that model the circuit. For each circuit node (logic gate), the table has an entry for the logic state (0, 1, X, Z) and, for each output of the gate, the list of input gates that are driven by this output gate. An event is said to have occurred when a signal changes state, and then is managed. The tool is described using C++, an object-oriented programming language. Each node of the circuit is modeled using a class.

The motivation of an in-house tool for simulation is related to the need of deeply understanding how the circuit reacts when a fault is injected. Standard commercial tools are usually optimized to reduce the execution time and they do not allow exploring all scenari required to really understand what is going on within the circuit.

For this same reason, the tool is now used for didactical purposes at the University of Montpellier and the ETS of Montréal (Canada). Moreover, ST Microelectronics is running some tests on the tool for evaluation.

The results of this work have been published in the papers [P13], [S17], [P17], [P27], [P32], [W17], [C13] referenced in the Publication list.

3.8. Test of 3D-Stacked Integrated Circuits

The stacking process of integrated circuits using TSVs (Through Silicon Via) is a promising technology that keeps the development of the integration more than Moore's law, where TSVs enable to tightly integrate various dies in a 3D fashion.

We started studying this topic in 2011 to address the new challenges related to the test of 3D-SIC (Stacked Integrated Circuits). The main challenges come from the novel levels of the fabrication process and the need for testing the circuits at the different phases (pre-, mid-, and post-bond tests). Pre-bond test targets the individual dies at wafer level, by testing not only classical logic (digital logic, IOs, RAM, etc,) but also unbounded TSVs. Mid-bond test targets the test of partially assembled 3D stacks, whereas finally post-bond test targets the final circuit. It is generally admitted that a 3D test flow should involve test procedures at all stacking levels of the 3D components including specific procedures for pre-bond TSV testing in order to provide Known Good Die before stacking.

We addressed two main problems. From one side, pre-bond testing of TSVs is a real issue due to the difficulty to get direct access to TSVs, which are not connected yet, using fine probe heads. So specific Design-for-Test structures for TSVs should allow to anticipate controllability and observability bottlenecks. From the other side, the classical Test Access Mechanisms implemented in current standards must be revised to follow the new production flow. Indeed, the test of a die requires dedicated I/O pad to bring test stimuli and to observe test responses. However, once the die is stacked to another die, the dedicated I/O pads are no longer available (because they are physically covered by the other die). Therefore, new Test Access Mechanisms must be defined in order to re-route test data from different input sources, to different output signals.

The next two sections focus on the recent works we carried out in the last two years. In particular, we have developed a solution for pre-bond test of TSV and we elaborated some new ideas to extend an on-going IEEE standard (IEEE P1687, IJTAG) to 3D-SIC circuits. This work is conducted in cooperation with the CEA-Leti (Grenoble).

3.8.1. 3D IC BIST for pre-bond test of TSVs

The underlying idea is that an unbound TSV can be electrically modeled by a RC network, whose main contribution is given by the capacitance connected to ground, as shown in Figure 2.18.

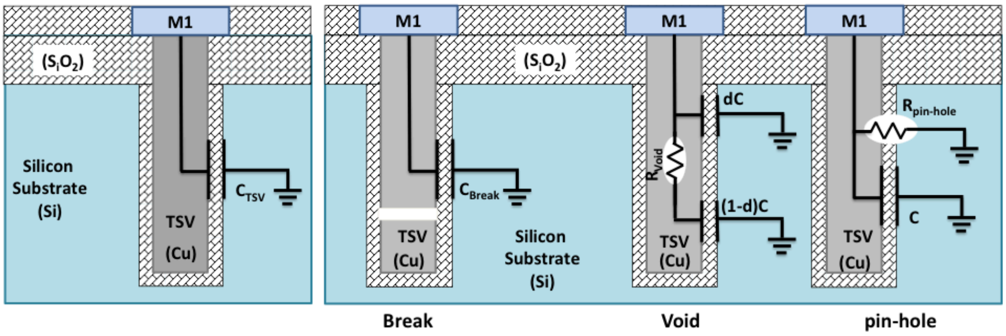


Fig. 2.18: TSV modeling

The main assumption in detecting defective TSVs is that a possible defect (pinhole, micro-void or broken TSV) would affect the delay of the RC network. By measuring this delay it would be possible to distinguish between good and faulty TSVs.

We have proposed a Built-In Self-Test architecture that allows measuring the dischargee time of the RC network. Fig. 2.19 gives an overview of the proposed BIST implementation for testing one TSV. The TSV Test Circuit is used to charge/ discharge and to sense the voltage level at the TSV top end. The Control signal monitors the different test phases. A Flip

Flop (FF) is used to store the OutSensing signal at the TSV Test Circuit output and delivers the TSV Test Result. Conversely to related works, the proposed DfT circuitry also includes a Delay Circuit that generates the sampling signal Clk used to store the test result of the TUT after an expected delay. Clk is slaved to the Control command.

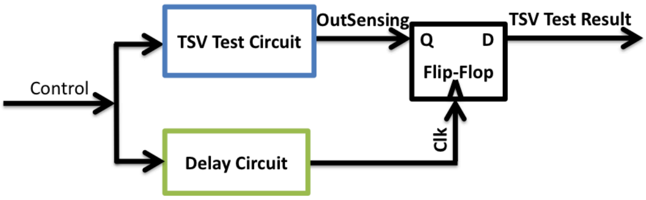


Fig. 2.19: Block Diagram of the Proposed BIST TSV Pre-Bond Test Scheme

Details of the TSV Test Circuit is given in Fig. 2.20. The TSV is represented here by a global model according to fault models presented in Fig. 2.18. A fault-free TSV is such that Rvoid=0, Rpin-hole = ∞ and the TSV equivalent capacitance is defined as dC+(1-d)C=C. Transmission gates are used to connect the TSV to the test circuitry or to the logic used in mission mode.

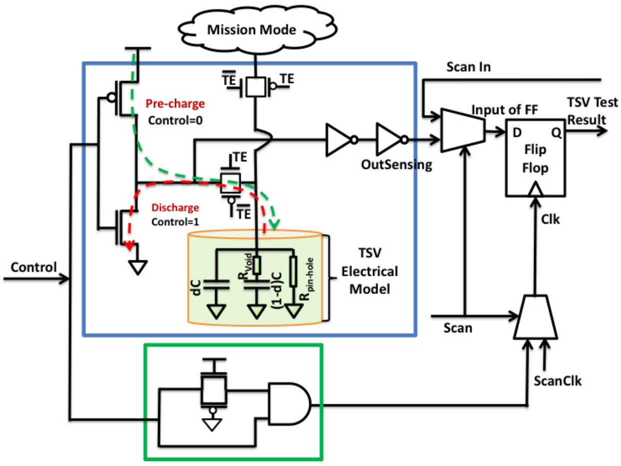


Fig. 2.20: BIST scheme for TSV Pre-Bond testing

The PMOS transistor of the inverter connected to the TSV top end is used to pre-charge the TSV to VDD when Control = 0. The TSV can also be discharged through the NMOS transistor by switching Control to 1. The two inverters on the right-hand side are used for TSV voltage sensing. After the pre-charge phase, the voltage level at the TSV top should be high enough to switch these two inverters and generate a logic ‘1’ on the OutSensing signal. After discharge, OutSensing should be equal to ‘0’. Charge and discharge times depend on the capacitance of the TUT and on possible extra serial resistance or leakage to the substrate.

The test procedure consists in charging the TSV and then to discharge it while sampling the voltage level just before that OutSensing falls to ‘0’ due to the TSV discharge. The BIST circuitry should capture the logic value ‘1’ in the FF for a fault-free TSV. In case of fault the discharge occurs sooner, OutSensing falls to 0 before the expected time and the BIST circuitry should capture ‘0’ (fail) instead of ‘1’ (pass).

Experimental simulation results shown that for small local variability (that is usual the case for even new technologies under 45nm), the measure of the discharge time is not sensitive to PVT variations, thus leading to a robust mechanism.

The results of this work have been published in the papers [C14], [S30], [P33], [P31], [C12] referenced in the Publication list.

3.9. Reliability of Microprocessor-based Systems

3.9.1. Watchdog for Reliability

VLSI and microprocessors performances have increased by more than five orders of magnitude in the last three decades, made possible by continued technology scaling. This trend will probably continue in then next years providing an integration capacity of billion of transistors. As technology scales further we will face new challenges, such as variability, single event upset (soft errors), and device degradation. All these effects manifest as inherent unreliability of the components posing design and test challenges.

I proposed an instruction checking methodology aiming at identifying the correct execution of each instruction on a microprocessor-based system during its normal behavior. The overall idea is to monitor a set of control signals of the target microprocessor identifying erroneous sequences of activations. The approach is able to identify both transient and permanent errors in the internal logic of a microprocessor that modify the activation sequence of the monitored signals.

Of particular interest of this work is the design of an algorithm able to identify the minimum set of signals to observe in order to obtain the required level of fault detection.

The main idea relies on the definition of an external hardware module (ICM: Instruction Checking Module) trying to understand if the currently executed instruction is exactly the one fetched from the system bus by observing a set of signals coming from the microprocessor.

Each instruction fetched by the microprocessor is also fetched by the ICM. The ICM observes a set of control and status signals coming from the microprocessor. Those signals can be either taken from the boundary or from the interior of the microprocessor when possible. By observing the waveforms produced by each executed instruction on the monitored signals and by comparing those waveforms with a set of pre-calculated ones obtained by simulation, the ICM is able to check the correct execution of the instruction.

The results of the work have been published in the paper [S17], referenced in the Publication list.

3.9.2. Evaluation of the Reliability of Microprocessor-based Systems

AS microprocessor technology scales down to the very deep sub-micron range, high production variability, voltage scaling and high operating frequency increase the hardware susceptibility to (soft) errors. This has a negative impact on the reliability of a wide range of computer-based applications which are critical to our health, safety and financial security. Since 1996 several studies reported cases of large computer system failures caused by cosmic-ray-induced soft-errors.

Several techniques have been proposed to protect digital circuits against soft-errors, e.g., radiation-hardened technologies, error detection/correction codes and redundant architectures. Software Implemented Hardware Fault Tolerance (SIHFT) also gained attention in the last decade. These techniques have a negative impact on systems' performance, power consumption, area and design complexity. Their application must therefore be carefully evaluated depending on the soft-error rate of the target system.

Unfortunately, tools and techniques to estimate the susceptibility of a computer system to soft-errors, taking into account both the hardware and the software domain, are not readily available or fully understood. The execution of a program may mask a large amount of soft-errors. In fact, at the system level soft-errors do not matter as long as the final outcome of the program is correct. To efficiently trade-off between fault tolerance cost and system reliability one has to ask: what is the probability of a program P to have a correct execution state given a certain hardware (raw) soft-error rate? Fault injection is a viable solution to answer this question. However, it can be very expensive and time consuming.

We have proposed a new methodology to estimate computer-based systems reliability against soft-errors. The target microprocessor is first characterized to profile the probability of successful execution of each instruction of its Instruction Set

Architecture (ISA). A static and very fast analysis of the control and data flow of the executed software is then performed to compute its probability of successful execution in case of soft-errors. The presented method has the potential to help engineers to choose the best hardware and software architecture to minimize the impact of soft-errors on the system's reliability.

In the context of this work, estimating the failure probability of a computer system running a program P means estimating the probability of observing an error in the outcome of the program (assumed bugs-free) running on a hardware system affected by soft-errors only. Soft-errors in the hardware may be masked either because they affect idle resources, or because the program's execution somehow overwrites the error. Based on this assumption, this section introduces an analytical model to estimate the probability of success of a program in presence of soft-errors in the hardware.

Programs are analyzed using the concept of program traces. A program trace is an ordered sequence of k instructions (k-tuple) executed while running a program. Two approaches can be followed to obtain a relevant set of traces for the proposed reliability estimation model. Whenever a strong, statistically relevant set of inputs for the target software is available, it can be exploited to derive a corresponding set of traces. Several runs of the program are executed, each with a different input, and run-time information about executed instructions and accessed data are recorded to compose each trace. The probability assigned to each trace can be uniformly distributed or calculated based on the knowledge of the probability of occurrence of the corresponding inputs. However, in several situations in which very early design exploration is performed, a statistically relevant set of inputs might not be available, or it might be difficult to estimate how much it covers the set of possible executions. For these situations, we proposed an algorithm that generates a set of traces by performing a static analysis of the program's binary code. The goal of the proposed algorithm is to cover as many parts as possible of the control-flow graph of the application, providing also a metric to measure how many of the possible paths have been covered.

In this algorithm, fault injection is used only once for a one-time, reusable, characterization of the microprocessor in terms of probability of success of each of its instructions in the presence of a soft-error in the hardware. The overall reliability of the microprocessor running a given workload is then computed with a purely probabilistic approach. The same characterization can then be reused every time the same CPU is used to build a new system or a new application software needs to be evaluated. The proposed method makes it possible to perform early exploration of design alternatives giving the possibility of comparing the system reliability using different processor architectures, even before the actual system's design is available.

We showed that the proposed method is extremely efficient with a high resolution. The results of the work have been published in the paper [J10].

4. Students

4.1. Master students

- Alessandro Dispenza (2001): A logic fault simulator implemented as self modifying code
- Ivano Solcia, Elisabetta Iorio (2002): A web-based tool for peer-reviews
- Fabrizio Micheletti (2002): Delay Fault Testing: a comparison among available tools and methods
- Claudio Marvaldi (2002): Circuit to automatically generate FPGAs' bitstreams for test purposes
- Alberto Bosio, Francesco Ciartiano, Ivano Picco (2003): SJAM Memory Test Pattern Generator
- Vincenzo Santoro, Francesco Sorace (2003): Code analysis methodology to characterize the termination probability of an application affected by a SEU in the binary code
- Andrea Bardone, Elisabetta Corsi (2003): An environment for fault injection based on a ethernet router in Linux
- Stefano Palazzo (2004): an ATPG for balancing the power consumption during the burn-in test
- Jean Paul Piccato (2004): Control Flow checking to protect microprocessors against radiations
- Paolo Pellegrino (2004): A watchdog process to increase the reliability of computer systems
- Gianfranco Panico, Piero Bellomo (2005): Self-Repair of FIR Filters
- G. Vezza (2006): Trusted Flow to protect against soft errors
- Bottigliero Davide, Magazzù Donato, Roviora Samuele (2006): Development of a e-learning platform (in cooperation with the UniNettuno university in Rome)
- Ignazio Cumbo (2006): Experimental modeling of ballistic applications via Finite State Machines
- Ana Agudo (2006): Audio/Visual remote systems using RTP protocol
- Ahmed El Boujouf (2008): A masking approach to protect AES against DPA
- Khalid Jettioui (2008): Identification of optimal input sequences for DPA
- Jihan Rezwan (2008): A fast approach for the identification of correlation between power and data
- Vincent Gregot (2008): Study and implementation of an attack platform for DPA
- Driss Aboulkassimi (2009): Validation of an optimization method for DPA attacks
- Miro Valka (Post-Master, 2010): Development of a tool for enhancing the resolution of the DPA
- Liang Shao (2011): Testing identical dies in 3D stacked Integrated Circuits
- Chloé Desdouits (2012): Implementation of an optimal algorithm for Wafer to Wafer matching
- Artem Marisov (2013): Implementation of a TMR scheme at flip-flop level

4.2. PhD Students

Table 4.1 summarizes the PhD students I co-directed, along with the period of the thesis and the percentage of supervision.

PhD Student	Years	%
Luca Tagliaferri	2003-05	10%
Alberto Bosio	2003-06	20%
Clara Tibaldi	2003-06	10%
Alessandro Savino	2005-07	10%
Marion Doulcier	2007-08	10%
Kaouthar Bousselam	2008-12	30%
Jean Da Rolt	2009-12	30%
Feng Lu	2011-	40%
Yassine Fkih	2011-	25%
Stephan De Castro	2012-	25%
Papa Sidy Ba	2013-	25%
Maha Kooli	2013-	70%
	Overall	305%

Table 4.1: Summary of the PhD Students

Luca Tagliaferri - "Source code modifications for on-line error handling"

The thesis is about a source to source compiler that is fed with C/C++ code and produces as output functionally equivalent to the one in input but enriched with routines and redundant code abler to detect errors injected within the program memory. The program itself was written with Microsoft Foundation Classes and the library engine was written partly in C and partly in C++.

The research aims at finding the possibility to realize software able to detect and possibly correct faults occurred during program execution and caused by external unauthorized agents. During the research many fault tolerant tools, library as well as a fault injection environments have been developed.

Alberto Bosio - Dependable Architectures for Safety-Critical Applications

Any new semiconductor technology provides further miniaturization and higher performances, increasing the number of advanced functions that electronic products can offer. Microcomputers are increasingly being used in applications where their correct operations are vital to ensure the safety of both people and the environment. These "safety-critical applications" include, among the other, anti-lock braking systems in automobiles, fly-by-wire aircrafts, shut-down systems in nuclear power plants. It is, therefore, vital that engineers be aware of the safety implications of the systems they develop.

There is a clear trend to integrate large quantities of memories on a chip. Memories are designed with aggressive design rules and tend to be more prone to manufacturing defects. Memories in complex SoC are deeply embedded in the circuits and are not easily accessible from the chip pin to apply test program. New IP Infrastructures to embed the test programs and to allow diagnosis and debug operation are required.

Furthermore, the increasing scale of integration and the introduction of new manufacturing processes introduce new classes of defects not present in the previous technologies. To efficiently deal with them, the process of memory test program generation should be automated to a maximum extent. This goal involves the realization of algorithms able to address the problem of: (i) describing new fault models (ii) generating tests able to cover these new fault models, (iii) verifying the effectiveness of the generated test programs.

This work leads to implement two methodologies to increase system dependability, tackling memory and processor testing, respectively, and a Fault injection environment used to evaluate the system dependability. In particular, a MArch Test automatic generator Engine (MaTE) has been developed. It can generate non-redundant March algorithm from user-defined fault lists. The generated test algorithm can be used in every test strategies, such as end-of-production test, BIST or On-line-test. Automatically generated test algorithms proved to be able to reduce the total amount of test time of more than 16% w.r.t. previously state-of-the-art techniques. Moreover, a functional test strategy for a generic microprocessor has then been designed; to prove the efficiency of the methodology a completely test suite procedures for the Motorola PowerPC 603 core has been implemented.

Clara Tibaldi: Test Access Methods for System-On-Chip

Progress in the System-on-a-Chip (SoC) technology and reuse methodologies have allowed integration of component from different sources into a single chip. For a SoC design consisting of multiple large cores, these core tests constitute a large part of the overall IC test. The emerging IEEE P1500 standard addresses the specific challenges that come with testing deeply embedded reusable cores supplied by diverse providers, who often use different hardware description levels and mixed technologies.

The work focused on the formal verification of core-wrapper P1500-Compliance with the purpose to assure that the component can be successfully integrated in a SoC. In addition, the P1500 Compliance Checking Environment (P1500 CCE) can assist the core suppliers in providing a CTL description of the core, create the CTL description of a P1500-Compliant wrapper for the unwrapped core, synthesize the relative VHDL wrapper, and suit the core test patterns for the wrapper.

Alessandro Savino: Software-based Self-Test of Microprocessor

System-On-Chip technology trends are so advanced that in a single chip one can embed different core, having different functionality, making possible the definition of the Intellectual Properties, such as microprocessor, memories and other peripherals. Microprocessor core testing becomes a very difficult task, due to the high complexity of internal architecture, moreover nature of an embedded core makes impracticable resort to classic external test mechanisms such Automatic Test Equipments. Rising of Built In Self Test (BIST) overcomes this problem porting the test mechanism and patterns inside the core. BIST solution usually requires to stop the core functionality in order to perform the test. However, critical applications require an on-line test executed in working condition (it means that the component is placed inside the environment where it will work since its lifetime). On-line test nature suggests the typical preferred approach: Software-Based Self-Test (SBST), where test patterns are the microprocessor instructions, provided by the Instruction Set Architecture.

The PhD thesis studied and investigates novel microprocessor test generation methodologies.

Marion Doulcier: Self-Test of Secure Devices

At the core of an electronic device offering digital security services is the cryptographic coprocessor that executes the cryptographic function. Such crypto-cores provide security services such as confidentiality, integrity, and authentication. The work developed during the PhD thesis aimed at providing efficient test solutions for possible physical failures on the electronic device implementing the cryptographic algorithm. Most of the work focused on the exploration of autonomous Built-In Self-Test techniques where the input test patterns were self generated by the secure circuit itself.

In classical BIST solutions for generic digital logic, storage elements are organized into scan chains and additional hardware is used for feeding the scan chains with pseudorandom test data, and sinking the test responses before analysis of the compressed signature. However, additional logic for BIST implementation can costly its (in terms of fault coverage and test length) can be not optimal. The thesis work demonstrated the efficiency of the autonomous generation of input sequences and the intrinsic collection of output responses.

Kaouthar Bousselam - Countermeasures against fault attacks in cryptographic circuits

To ensure confidentiality and secure data exchanges, secure circuits use cryptographic certified algorithms. Despite this, the attackers have not stopped looking for possible ways in order to retrieve the secret data processed by these circuits. One powerful method is to inject a fault in the circuit during normal operation. This fault will produce an incorrect result at the output of the circuit. Comparing correct result (i.e., without fault injection)and wrong result (i.e., with fault injection), the attacker can extract information about the secret data processed by the circuit.

The aim of Kaouthar's thesis has been to improve the strength and reliability of security against attacks at fault circuits. To achieve this goal, she worked on the online detection of errors by using advanced error detection codes. Moreover, rather than detect all kinds of errors, she focused on the detection of realistic errors that may be produced by such attacks. She defined a fault model and, based on that fault model, she found the best error detection codes that cover errors generated by those faults.

I was a member of her thesis defense jury.

Jean Da Rolt - Testability vs. Security: New Scan-Based Attacks & Countermeasures

Jean firstly analyze the vulnerabilities induced by test infrastructures onto embedded secrecy in digital integrated circuits dedicated to cryptography. Then he proposed new scan-based attacks and effective countermeasures. Scan chains insertion is the most used technique to ensure the testability of digital cores, providing high fault coverage. However, for ICs dealing with secret information, scan chains can be used as back doors for accessing secret data, thus becoming a threat to device's security. We start by describing a series of new attacks that exploit information leakage out of advanced Design-for-Testability structures such as response compaction, X-Masking and partial scan. Conversely to some previous works that proposed that these structures are immune to scan-based attacks, we show that our new attacks can reveal secret information that is embedded inside the chip boundaries. Regarding the countermeasures, he proposed three new solutions. The first one moves the comparison between test responses and expected responses from the Automatic Test Equipment to the chip. This solution has a negligible area overhead, no effect on fault coverage. The second countermeasure aims to protect the circuit against unauthorized access, for instance to the test mode, and also ensure the authentication of the circuit. For that purpose, mutual-authentication using Schnorr protocol on Elliptic Curves is implemented. As the last countermeasure, he proposed that Differential Analysis Attacks algorithm-level countermeasures, such as point-blinding and scalar-blinding can be reused to protect the circuit against scan-based attacks.

I was a member of his thesis defense jury.

Feng Lu - Transient Fault Simulation of Secure Devices

Secure devices (i.e. devices implementing cryptographic functions and/or storing secret information) are designed with the ability to protect information against unauthorized access and intentional misuse. For that, they implement state-of-the-art cryptographic algorithm that have proved to be resistant against cryptanalysis.

Unfortunately, when the algorithm is implemented in a hardware device, other types of attacks are possible. Among all the type of attacks targeting the hardware (also known as Side-Channel Attacks), one of the most efficient is the one based on the intentional injection of faults within the circuit. This type of attack, called "Differential Fault Analysis" (DFA), consists in inferring the secret data by comparing the results of a faulty and a fault-free encryption.

The first goal of this thesis is to understand and to model the behavior of a real fault injection on the circuit. After understanding the type of faults that can be injected on a circuit, the second goal of the thesis is to develop a transient fault simulator able to reproduce the behavior of a circuit under attack. The simulator, that is under development, is able to deal with gate-level netlist with timing information of each port, and it can consider its layout (i.e. the topological information of each gate within the circuit).

Yassine Fkih - Test of 3D Stacked Integrated Circuits

TSV-based 3-Dimensional (3D) integrated circuit is an emerging integration technology where multiple layers of planar devices (dies) are stacked and interconnected using so called Through Silicon Vias (TSVs). Multiple dies are stacked vertically, significantly increasing on-chip device count thus extending Moore's Law. Besides footprint advantages, the potential benefits of 3D integration can include higher device speed, smaller overall cost, lower power consumption, larger bandwidth, and it will allows heterogeneous designs.

Unfortunately, 3D die stacking also presents new challenges. Among them, test and testability is a chief challenge. In particular, new defects can appear during the bonding process (defects that are not modeled for single-die technology), fault models in TSV are not yet fully modeled, test strategy (i.e., pre-, mid-, and post-bond test) must be specifically defined to cope with this fabrication process, and test access mechanism become more complex due to the limit access the inter-dies.

The main objective of this PhD thesis is the study of the specific issues related to the 3D integration technology that impact the test and the testability of the whole system. The work is covering the following aspects: to develop different test strategies according to the available test resources and the assembly process; to understand and define the best test strategy (i.e., which fault must be tested at which test step) to allow the best trade-off between yield and test cost; to analyze the issues arising from limited test access to the components of the 3D circuit w.r.t current definition of new standards.

Stephan De Castro - Laser-Induced fault Effects in Security-dedicated circuit

Modeling and Simulation of Laser Attacks against secure circuits Secure devices (i.e. devices implementing cryptographic functions and/or storing secret information) are designed with the ability to protect information against unauthorized access and intentional misuse. For that, they implement state-of-the-art cryptographic algorithm that have proved to be resistant against cryptanalysis. Unfortunately, when the algorithm is implemented in a hardware device, other types of attacks are possible. Among all the type of attacks targeting the hardware (also known as Side-Channel Attacks), one of the most efficient is the one based on the intentional injection of faults within the circuit. This type of attack, called "Differential Fault Analysis" (DFA), consists in inferring the secret data by comparing the results of a faulty and a fault-free encryption.

The first goal of his thesis is to understand and to model the behavior of a real fault injection on the circuit. Stephan is currently study the effect of real experiments performed by using laser attacks on both the backside and the frontside of the integrated circuit. After understanding the type of faults that can be injected on a circuit and after having developed comprehensive fault models exploitable at logic level, the second goal of the thesis is to integrate the faults into the simulator under development in our group.

Papa Sidy Ba - Hardware Trojan Detection

The vulnerabilities in today's design and fabrication process have raised the possibility of malicious circuit insertion into an integrated circuit to impact its functionality or transmit secret key information to the adversary. Such malicious circuits are known as Hardware Trojans Horses. Hardware Trojan detection problem has gained significant attention over the past few years and is becoming a major concern specifically for secure devices.

Among others, one way to guarantee the absence of such trojans is defined Trojan models that can be represented as additional gates in the circuit, and to generate test patterns targeting those additional gates. The goals of this thesis are, first to propose innovative methods to identify possible locations of the Hardware Trojans, and then to provide solutions for generating suitable test vectors able to detect them.

Maha Kooli

Information technology is at the core of our society and it relies completely on the design of electronic information processing systems. Today's computing is a true continuum that ranges from smart-phones to mission-critical datacenter machines, and from desktops to automobiles. Therefore, reliability of electronic systems becomes a key challenge for the whole information and communication technology and must be guaranteed without penalizing or slowing down the characteristics of the final products.

In this context, the FP7 project CLERECO aims at addressing the problem of having an early, fast, and accurate evaluation of computing systems reliability to support design decisions for hardware and software reliability enhancing mechanisms in the system. Such solutions can be only developed if the expected reliability of the system can be quickly and accurately assessed: (a) at different stages of the design flow (from design concept and early design stages through first silicon validation and eventually during operation in the field), (b) considering the impact of all hardware and software components, and the different modes of operation (use cases) of the system. Finally, the development of a reliable and dependable product that employs mechanisms to detect and handle possible faults can reduce the overall life cycle costs.

The goals of the work that will be performed by the PhD student are: to analyze the reliability of the different hardware and software components at different levels of detail (depending on the design phase), emphasizing the role that the interaction between hardware and software plays in the overall reliability figure of the system; to validate the reliability of the system via a flexible, fast, and accurate evaluation framework; to comprehensively support the reliability decision-making process in computing systems with a reliability evaluation framework (methodology and tools) that leads to just the right reliability for the system.

4.3. PostDoc Students

Rodrigo Possamai Bastos

The semiconductor industry is one of the enablers of new businesses. General usage of products such as mobile phones, and GPS navigation are only made possible by the constant cost-down of the manufacturing of a single transistor as well as the integration of digital, analogue and RF blocks in a single package. This cost down trend will continue. This provides opportunities for new products such as car radars that will improve safety and comfort of Europeans but only if test solutions exist that match the silicon cost-down.

The objective of this PostDoc is to achieve this cost-down by developing and deploying innovative, cost-effective test solutions for integrated circuits that meet the constantly increasing quality requirements. The cost-effective part should surpass the cost down on the manufacturing side of these products as ensured by Moore's law, while the improved quality levels should surpass those set by industry.

Hardware implementation of dedicated functions and co-processors allows performance improvement compared to software solutions; however, a hardware fault may jeopardize the reliability of the device. In addition, digital circuits become more and more sensitive to aging phenomenon, SEUs and SETs due to dimension shrinking in new technologies.

The particular goal of the post-doctoral work performed by Rodrigo was threefold: Investigation of test procedures for hardware implementation of co-processing functions; Development of dedicated concurrent fault detection techniques for specific co-processors; Development of new solutions for resistance against transient and permanent faults

Hakim Zimouche - Pre Bond Test of TSVs

The work of Hakim was complementary to the one of Yassine Fkih. He also addressed the pre-bond test of TSVs, with a particular focus on a Built-In Self-Test method to measure the delay of the RC network (including the TSV) that does not rely on ring oscillator.

He designed a Built-In Self-Test architecture that allows measuring the dischargee time of the RC network where the expected delay was obtained by a full-custom implementation of a delay network composed of NAND gates.

5. Teaching activities

Starting from my Ph.D. studies, I have performed various teaching activities at different levels: engineering students of the Politecnico di Torino and the Engineering School of the University of Montpellier 2, master students of the military school of the University of Torino, students of private institutions, as well as embedded tutorials on specific scientific topics in international conferences.

The topics of my teaching activities (focusing on academic courses only), as well as the description of the course and the targeted students are described in the following paragraphs:

- **Computer Sciences**: this class introduces the student to the issues related to computer science and it aims at teaching the use of computer programming using the C language.
    - Covered topics: Data types, Symbolic constants, Input/output operations (printf and scanf), Control-Flow structures (iterative and conditional), Arrays and multidimensional arrays (of integers, reals and characters), Functions and calls (by reference, by value, pointers), Strings, Command line arguments (argc and argv), Files, Struct, Dynamic memory allocation.
    - When, where, for who:
        - 2000/01, 2001/02, 2005/06, Politecnico di Torino, Computer Engineering students
        - 2008/09, 2009/10, 2010/11, 2011/12, Polytech' Montpellier (Université de Montpellier II), Electronic Engineering students
- **Advanced Computer Sciences**: this class introduces classical algorithms, data structures and problem-solving paradigms in C.
    - Covered topics: Complexity analysis, Elementary data structures: stacks, queues, lists, Abstract data types, Problem-solving paradigms: divide and conquer, dynamic programming, Recursion, Sorting algorithms, Graphs theory.
    - When, where, for who:
        - 2001/02, 2002/03, 2003/04, 2004/05, Politecnico di Torino, Computer Engineering students
- **Computer Architecture**: this class introduces the basic information about the architecture of a computer system.
    - Covered topics: CPU architecture, Assembly level programming languages, arithmetic units, memories and memory management systems, peripheral devices and their management (serial and parallel port interfaces, timers, interrupt and DMA controllers), communication structures.
    - When, where, for who:
        - 2005/06, Politecnico di Torino, Computer Engineering students
        - 2008/09, 2009/10, 2010/11, 2011/12, 2012/13, 2013/14, Polytech' Montpellier (Université de Montpellier II), Electronic Engineering students
- **Databases**: this class provides the knowledge of databases in terms of conceptual design and management rules, with the focus on relational model.
    - Covered topics: Relational model - Relational algebra, SQL: data definition language and data management language, Transactional systems and failure management, Conceptual data model - Entity/Relationship model, Techniques for designing a conceptual schema, Techniques and tools for designing a logical-relational schema, Normalization theory
    - When, where, for who:
        - 2000/01, 2001/02, 2004/05, 2005/06, Politecnico di Torino, Computer Engineering students
        - 2012/13, 2013/14, Polytech' Montpellier (Université de Montpellier II), Electronic Engineering students
- **Operating Systems**: this course introduces the concurrent programming techniques and the architecture of operating systems, with particular emphasis on system resources and system programming. The Linux operating system is used as a case study for analysis.

    - Covered topics: Architecture of operating systems, Different forms of kernels, Sequential and concurrent processes, Process status, domain and context-switching, UNIX system call for process handling, Process synchronization, Event flags, signals, semaphores, IPC, System management: commands and shell scripts and filters
    - When, where, for who:
        - 2000/01, 2001/02, 2002/03, 2006/07, Politecnico di Torino, Computer Engineering students
        - 2007/08, 2012/13, 2013/14, Université de Montpellier II, Electronic Master students (focus on “Commands and shell scripts and filters” only) and Polytech Montpellier
- **Automatic Processes**: this course provides basics on automatic control systems, including analysis and design of feedback control loops.
    - Covered topics: Introduction to control systems: open- and closed-loop control systems, uncertainties and disturbance signals in feedback control systems, Frequency response analysis: Bode, polar and Nyquist plots, Stability of linear feedback systems: Nyquist criterion and stability margins.
    - When, where, for who:
        - 2004/05, 2005/06, Università di Torino, Strategic Science master students
- **Digital System Testing**: The course aims at showing the importance of testing within the design and manufacturing process. It presents the techniques for testing custom Integrated Circuits, microprocessors, memories, and system test.
    - Covered topics: Fault modeling, understanding of the tools for testing an embedded system: fault simulator, automatic test pattern generator, tools for automatic scan chain insertion. Concept of Built-In Self-Test (BIST).
    - When, where, for who:
        - 2006/07, Politecnico di Torino, Computer Engineering students
        - 2008/09, EMSE Gardanne, Master SISA Students
        - 2012/13, Polytech Montpellier
- **Tutorial on “Test and Security”**: Cryptographic algorithms are used to protect sensitive information from untrusted parties when the communication medium is not secure. Many secure systems such as smartcards include hardware implementation of symmetric cryptographic algorithms such as (Triple) Data Encryption Standard and Advanced Encryption Standard. The secret keys used to encrypt the data with these algorithms are large enough to prevent any brute force attack that consists in exploring the whole solution space (2n with 64<n<256). However, the hardware implementation of these cryptographic algorithms allows the hackers to measure the observable characteristics of the physical implementation and deduce the secret key (side-channel attacks). The key can even be discovered by applying a side-channel attack on scan chains. These scan chains, which aim to provide full controllability and observability of internal states, represent nevertheless the most popular design- for-testability scheme. Because crypto-processors and others cores in a secure system must pass through high-quality test procedures to ensure that data are correctly processed, testing of crypto chips faces a dilemma: how to develop a design-for-testability scheme that provides high testability (high controllability and observability) while maintaining high security (minimal controllability and observability)? This tutorial presents the security weaknesses generated by scan designs on hardware AES and DES implementations. It also discusses the pros and cons of security-dedicated DFT, BIST and Fault tolerance solutions taken from the literature.
    - Covered topics: Test & security: antagonism, Scan-based approach, BIST approach, Fault tolerance.
    - When, where, for who: this course has been presented as embedded tutorial (90 minutes for an international audience of engineers and researchers) during the following international events:
        - 2009, IEEE Latin America Workshop (LATW’09)
        - 2009, IEEE European Test Symposium (ETS’09)
        - 2010, IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS’10)

6. Funded Projects

Starting from my Ph.D., I have actively cooperated to national- and european-funded scientific projects. In some cases I have contributed in the redaction of the project proposal (GRAAL, TestDOC, TReDiCo, Liesse, CLERECO, TRUDEVICE). Some details concerning each project are presented in the next sub-sections, following a chronological order.

Giovani Ricercatori

Title: Development of a software environment for highly dependable space applications

Place and period: 2000-2002, Politecnico di Torino

Funding: framework of the "Giovani Ricercatori" (Young Researchers) project within Politecnico di Torino (50K€)

Goal of the project: development of new methodologies to increase the dependability of space applications using software techniques. the software fault tolerance aims at addressing system failures caused by a hard or soft error appearing in the system hardware. The main results of this project have been, from one side, an ad-hoc Source-to-Source C++ compiler able to transforms any input C/C++ source code into an output C/C++ reliable code, properly modified to increase its dependability characteristics, and, from the other side, a proprietary Fault Injection tool running under Windows NT 4.0.

Contribution and results: my contribution in this project was the introduction of some methodologies to increase the reliability of the system in a source-to-source compiler ([W6], [S8]) and the development of the fault injection tool ([W9]).

GRAAL

Title: Generatore di celle RAM ad Altissima Affidabilità per applicazioni Life e safety-critical (Tool for Highly Dependable SRAMs Generation)

Place and period: 2001-2003, Politecnico di Torino

Participants: Aurelia Microelettronica (project leader), Politecnico di Torino, Università degli Studi di Pavia, ERMEC, ABEL s.r.l.

Funding: project S167P founded by the Italian Ministry of the University and Technological and Scientific Research (720M€)

Goal of the project: using GRAAL, the designer can define a dependable SRAM architecture, which achieves the target dependability requirements and design constraints. The dependable SRAM architecture is designed in order to guarantee high reliability levels. It includes the Built-In-Self-Test (BIST) logic for memory testing: it allows testing the memory using OFF-line and/or ON-line testing strategies. In the case of ON-line testing, the implementation of both Concurrent and Not-Concurrent test strategies is supported. Moreover, the dependable SRAM architecture can also include the Built-In Self Repair (BISR) logic for functional memory repairing.

Contribution and results: my contribution in this project was the definition of the reliable SRAM architecture and, in particular, the design of proper BIST and BISR schemes. Results of the project have been published in [C5] and [S18].

Test DOC

Title: Test Doc, Quality and Reliability of Complex Systems-on-Chip

Place and period: 2001-2003, Politecnico di Torino

Participants: Politecnico di Torino (project leader), LIRMM, Universitat Politècnica de Catalunya, Siemens ICN, LogicVision, Virage Logic

Funding: Istituto Superiore M. Boella, www.testgroup.polito.it/tdoc (1200M€)

Goal of the project: the project aimed at defining new Design for Testability (DfT), Built -In Self-Test (BIST), and Built-In Self-Repair (BISR) techniques to improve the quality and dependability of System-on-Chips (SoCs). The research addressed both the general problem of planning and implementing a global test strategy for SoCs, and the specific problem of defining effective DfT, BIST, and BISR architectures for different types of commonly used digital cores as FPGAs, Memories, and microprocessors. Two industrial demonstrators have been implemented to show the applicability and the effectiveness of the techniques defined during the project.

Contribution and results: Leader of the Work Package 2 - Task 1 (“BISR for SRAM memories”). Results of my contribution have been published in [J3] and [J4].

TReDiCo

Title: Testable and Reconfigurable Digital cores

Place and period: 2004-2006, Politecnico di Torino

Participants: Politecnico di Torino, Institute of Informatics of the Slovak Academy of Sciences

Funding: Ministry of Education of the Slovak Republic and Ministry of the University and Technological and Scientific Research, under the “Slovak – Italian Science and Technology Co-operation for years 2004 – 2007” program

Goal of the project: the project was aimed to research in the area of advanced testability and built-in self-test algorithms and methods with self-healing features and their application to digital cores. The goal is to design and implement efficient techniques for testability and reconfigurability applied into the digital cores.

Contribution and results: results of my contribution have been published in [C19], [C24] and [W25].

CALISSON

Title: Characterisation, Modelling and Security Specifications of integrated prototype circuits (“Characterization, Modeling, and Security Specifications of integrated prototype circuits”)

Place and period: 2007-2010, LIRMM

Participants: LIRMM, Atmel, CEA, Ecole des Mines in St Etienne, Gemalto, ParisTech, PSI Electronics, STMicroelectronics

Funding: FCE contract funded by the General Directorate for Competitiveness, Industry and Services (DGCIS) and it is sponsored by the "Secure Communications Solutions" competitiveness cluster

Goal of the project: the aim is to strengthen the security of electronic components by developing new means of secured characterization while designing integrated circuits, in order to reduce the overall cost related to security aspects.

Contribution and results: my contribution in this project has been related to the definition of a methodology that allows designers of secure devices to reduce the time required to validate a counter measure against side-channel attacks (in particular differential power analysis). Results of the project have been published in [S40], [W54], [S59] and presented in [P47], [P49], [P57], [P62].

TOETS

Title: Towards One European Test Solution (TOETS)

Place and period: 2008-2011, LIRMM

Participants: NXP, Infineon, Philips, Q-Star Test, Semicon, STMicroelectronics, Temento, iRoC, ATMEL, E2V Semiconductor, JTAG Technologies, Salland Engineering, Advan- ced Digital Design, Tomorrow Options Microelectronics, Ophtimalia, CEA-LETI, CEA-LIST, University of Twente, LIRMM, TIMA, KULEUVEN, SUPELEC, IMSE-CNM, INESC Porto

Funding: European Project CATRENE CT302 (more than 1M€ for the LIRMM)

Goal of the project: has the ambition to create a breakthrough in methods and flows used by the test technologies by considering the test in the whole value chain from Design to Application. It faces the giga-scale complexity of SoC with various and numerous implemented functions (RF, analogue, digital, memory), for which test becomes an economical roadblock. Its objectives are the definition of test architectures for minimizing the costs of test operation, to develop alternative test solutions and test flows for test cost reduction and product quality improvement. TOETS is geared toward the secure and safety critical application domain (consumer and medical).

Contribution and results: my contribution in this project deals with on-site testing of digital secure devices (WorkPackage 1.1). I cooperated in the definition of a Built-In Self-Test method that allows high fault coverage while guaranteeing the non violability of the secret stored in the secure device. Results have been published in [J8], [J9], [W34], [S42], [C52] and presented in [P36], [P37], [P45].

ProSecure

Title: Pro Secure

Place and period: 2010-2013, LIRMM

Participants: Cortus, INVIA, LIRMM, IM2NP

Funding: Languedoc-Roussillon region and Oseo (more than 1.4M€)

Goal of the project: to develop a new 32-bit embedded secure RISC processor which integrates all protections needed to make the system resistant to all kinds of attacks (e.g., faults, timing, reverse engineering, side channel). The microprocessor will respect tight constraints in terms of area and power consumption in such a way it will be possible to use it in applications like smart cards.

Contribution and results: the contribution of the LIRMM will focus the definition of test strategies that allow detecting the highest number of faults while respecting the constraints related to the security (Work Packages 2 and 6). Results of the project have been published in [J18], [J16], [J15], [J13], [J12].

CALISSON 2

Title: Characterisation, Modelling and Security Specifications of integrated prototype circuits 2 (“Characterization, Modeling, and Security Specifications of integrated prototype circuits”)

Place and period: 2011-2014, LIRMM

Participants: Gemalto, Inside, CEA LETI, LIRMM, Ecole des Mines in St Etienne, Oridao, PSI Electronics, STMicroelectronics, Telecom ParisTech

Funding: FCE contract funded by the General Directorate for Competitiveness, Industry and Services (DGCIS) and it is sponsored by the "Secure Communications Solutions" competitiveness cluster (1.8M€)

Goal of the project: the project aims to improve the security of integrated circuits for the IC market providing security functions like Smart Card, Digital Passport, or One Time Password. The ambition of CALISSON 2 is twofold. From one side it targets the improvement of the attack models developed during the CALISSON project by analyzing aggressive technologies beyond 65nm; from the other side, the project will develop a methodology to automatically insert in the design flow all the techniques and architectures proposed in CALISSON in order to reduce the cost related to the design of secure integrated circuits.

Contribution: Development of a simulation)-based fault injector tool and design of a countermeasure based on integrated sensor in the bulk of the circuit (BBICS: Bulk Built-In Current Sensor). Results of the project have been published in [J17], [J14], [J11], [P35], [W18].

LIESSE

Title: Laser-Induced fault Effects in Security-dedicated circuitS

Place and period: 2012-2016, LIRMM

Participants: LIRMM (project leader), ST, Ecole des Mines in St Etienne, LCIS, TIMA, ONERA

Funding: ANR, program “Ingénierie Numérique & Sécurité” (600 K€)

Goal of the project: the project focuses on countermeasures against fault attacks. Several papers have been published on such attacks, but mainly from a theoretical perspective i.e. by assuming some characteristics of the errors due to the injected faults. For instance, if it is supposed that one is able to change the value of a given bit at a given moment, then it is shown that it is possible to derive the secret key used during an encryption. Conversely, relatively few studies have shown the actual possibility to inject such appropriate faults in a circuit (i.e. with the expected characteristics) and especially onto deep-submicron technology circuits (65 nm, 40nm and 22 nm technologies). The main goals of this project are to study and model the effect of laser shots onto submicronic circuits and to provide efficient tools to circuit designers to prevent such laser attacks.

Contribution: fault modeling of laser effects (on both front- and back-side of the circuit), enhancement of the fault simulator developed in the CALISSON 2 project to consider geometrical and physical parameters. Preliminary results of the project have been published in [C13].

HOMERE

Title: Hardware trOjans: Menaces et RoubustEsse de ciRcuits intEgrés

Place and period: 2012-2015, LIRMM

Participants: Cassidian Cybersecurity (project leader), Secure-IC, Gemalto, ANSSI, ARMINES, CEA-LETI, LIRMM, Telecom ParisTech

Funding: FUI13 - OSEO - SYSTEMATIC PARIS-REGION (value of the project: 5M€, funding: 2M€)

Goal of the project: this project targets industrial research problems and it deals with the development of new methods to counteract possible Hardware Trojans. An important constraint that will be respected in the project is the definition of non-invasive methods that do not destroy the circuit to detect the presence of Trojans (like reverse-engineering).

Contribution: this project belongs to a trans-domain context for our group. The detection of possible Hardware Trojans will be addressed through techniques and methods that are generally used for the manufacturing testing of the integrated circuits. This topic will be more detailed in Chapter 3 (Perspectives).

MASTER 3D

Title: MAnufacturing Solutions Targeting competitive European pRoduction in 3D (MASTER 3D)

Place and period: 2012-2015, LIRMM

Participants: Air Liquide Electronics Systems, Austriamicrosystems, AXO DRESDEN GmbH, CAMTEK, CAMTEK LTD, Doublecheck Semiconductors GmbH, DR Yield, EV Group, Fogale Nanotech, GLOBALFOUNDRIES, ISIS sentronics GmbH, MASER Engineering, Mentor Graphics MAD/Micred, Nanda Technologies GmbH, NXP Semiconductors Germany GmbH, Presto Engineering Europe, PVA TePla, QUALTERA SAS, Rockwood Wafer Reclaim SAS, SILTRONIC AG, SOITEC, SPTS, STMicroelectronics Crolles SAS (project leader), ST-Ericsson, Budapest Univ. of Technology & Economics, CEA, Fraunhofer Gesellschaft, IMS Bordeaux, LIRMM.

Funding: CATRENE European Project

Goal of the project: The MASTER_3D project will contribute to transforming EU leadership in R&D of 3D Integrated Circuits into 3D IC manufacturing leadership. Manufacturing methods to maximize process robustness and yield, minimize ramp-up time, support high volume production and reduce manufacturing cost will be developed and implemented in the consortium FABs. The activities will focus on 3D ICs with Through Silicon Vias (TSV) and Wafer Level Packaging (WLP). Manufacturing Excellence will be addressed by: tool enhancements to support high yield, mass production; novel 3D Wafer Parametric Test, Functional and Final Test concepts; Characterization and in-line Metrology methods development.

Contribution: 3D Test Pattern Generation, Pre-bond testing of TSVs. Results of the project have been published in [C14], [S30], [P33], [P34], [W16], [C12].

COST Action TRUDEVICE

Title: Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)

Websites:

- www.trudevice.com
- http://www.cost.eu/domains_actions/ict/Actions/IC1204

Place and period: 2012-2016, LIRMM

Particularity: this project is a network of excellence that groups 22 countries in Europe and more than 60 entities (universities, research centers, industrial companies). The overall value of the project is 88M€. For this project, I am the action chair (i.e., project leader). Within the contest of TRUDEVICE, we organized 1 workshop, 1 working group meeting, and we will organize 2 workshops in 2014, a summer school and a workshop in 2015.

Funding: Europe COST (600K€)

Goal of the project: Hardware security is becoming increasingly important for many embedded systems applications ranging from small RFID tag to satellites orbiting the earth. Its relevance is expected to increase in the upcoming decades as secure applications such as public services, communication, control and healthcare will keep growing. The vulnerability of hardware devices that implement cryptography functions (including smart cards) has become the Achille's heel in the last decade. Therefore, the industry is recognizing the significance of hardware security to combat semiconductor device counterfeiting, theft of service and tampering. This COST action aims at creating a European network of competence and experts on all aspects of hardware security including design, manufacturing, testing, reliability, validation and utilization. The network will play a key role in developing solutions responding to the hardware security challenges, hence strengthening the position of Europe in the field.

CLERECO

Title: Cross-Layer Early Reliability Evaluation for the Computing cOntinuum (CLERECO)

Website: www.clereco.eu

Place and period: 2013-2016, LIRMM

Grant agreement no: 611404

Participants: Politecnico di Torino, LIRMM, University of Athens, Thales, Intel, ABB, Yogitech

Particularity: for this project I am the scientific leader for LIRMM.

Funding: FP7 Strep Project (value of the project: 4M€, funded: 2.5M€)

Goal of the project: CLERECO research project recognizes early accurate reliability evaluation as one of the most important and challenging tasks throughout the design cycle of computing systems across all domains. In order to continue harvesting the performance and functionality offerings of technology scaling, we need to dramatically improve current methodologies to evaluate the reliability of the system. On one hand, we need accurate methodologies that reduce the performance and energy tax paid to guarantee correct operation of systems. The rising energy costs needed to compensate for increasing unpredictability are rapidly becoming unacceptable in today's environment where energy consumption is often the limiting factor on integrated circuit performance. On the other hand, early "budgeting" for reliability has the potential to save significant design effort and resources and has a profound impact on the TTM of a product. CLERECO addresses early reliability evaluation with a cross-layer approach across different computing disciplines, across computing system layers and across computing market segments to address reliability for the emerging computing continuum. CLERECO methodology will consider low-level information such as raw failure rates as well as the entire set of hardware and software components of the system that eventually determine the reliability delivered to the end users. The CLERECO project methodology for early reliability evaluation will be comprehensively assessed and validated in advanced designs from different applications provided by the industrial partners for the full stack of hardware and software layers.

Contribution: the project just started. A PhD student is currently performing a comprehensive analysis of the literature.

7. Cooperations

7.1. Universities

Paolo Prinetto, Alfredo Benso, Silvia Chiusano, Stefano Di Carlo (Politecnico di Torino): Paolo, Alfredo and Silvia have been my PhD supervisor. Stefano (who made the PhD studies at the same time as me) shared many research topics with me, leading to several publications. The cooperation lasted also after moving to LIRMM, by keeping on developing techniques for the evaluation and the improvement of the reliability of a system.

Matteo Sonza Reorda (Politecnico di Torino): we shared for 4 years (from 2009 to 2013) the coordination of the European section of the Test Technology Technical Council. Matteo was the chair of the eTTTC while I was the vice-chair.

Guy Gogniat (Université de Bretagne-Sud): we shared for 4 years (from 2009 to 2013) the coordination of the working group "Security of Digital Embedded Systems" of the GDR SoC-SiP. Guy was the chair of the working group while I was the vice co-chair.

Paolo Maistri (TIMA Lab): we presented together a tutorial titled "Test & Security" during the European Test Symposium 2009.

Sybille Hellebrand (Univeristy of Paderborn): we cooperated to join our knowledge of test and repair of memories. The result of the cooperation has been two common papers ([S16] and [P11]).

Elena Gramatova (Institute of Informatics of the Slovak Academy of Sciences, from 2004 to 2006): in the context of the TReDiCo project, we developed a method for the built-in generation of test vectors for delay faults ([P2]).

M. Hosseinabady, Z. Navabi (University of Tehran, Iran from 2006 to 2007): we developed a new approach for the soft error evaluation based on the use of the UML for the model of the target system ([S9] and [S13]).

Ilia Polian (University of Passau, from 2012): Ilia is the vice chair of the COST Action TRUDEVICE and we often cooperate in order to lead the Action. Moreover, always in the context of TRUDEVICE, one of my PhD student (Feng Lu) spent 3 weeks at the University of Passau to improve the quality of his fault simulator.

Said Hamdioui (TU Delft, from 2012): Said is actively involved in the TRUDEVICE COST Action. Moreover, we are planning a common proposal for an Horizon 2020 project on security.

Ingrid Verbauwhede (Catholic University of Leuven, from 2012): we started a cooperation in the field of the test and security, and in particular in the definition of a protocol-based test access mechanism that allows protecting secure circuits from scan attacks. We published several common papers ([J18], [J15], [J12], [S27], [W15]).

Jean Max Dutertre (ENMSE, from 2008): we started a shared research activity with the CALISSON project, followed by CALISSON 2 and LIESSE. We have currently designed a CMOS circuit implementing the BBICS (Bulk Built-In Current Sensor). Moreover, we co-supervise the PhD student Stephan De Castro. We published some common papers ([J17], [P35], [W18], [S28]).

7.2. Companies

Pascal Vivet (CEA, from 2011): this collaboration started with the MASTER 3D project and the co-supervision of the PhD student Yassine Fkih. We published some common papers ([P34], [W16],[C12]) and we realized a patent.

Schloeffel Juergen (Mentor Graphics, from 2013): together with Pascal Vivet we defined a novel test access method based on IJTAG for 3D circuits. We recently made a common presentation [P34] and submitted a paper.

Riccardo Mariani (Yogitech, from 2001): this cooperation lasts from many years. I worked with him on memory testing in the framework of the GRAAL project. After that, we designed together a watchdog process to increase the reliability of automotive applications. We are currently working together in the context of the CLERECO project. We published some common papers ([S17] and [P1]).

Denis Real (DGA, 2008): we cooperated in the framework of the development of a DPA tool analysis [W14].

Monica Lobetti Bodoni (Siemens, from 2001 to 2003): the cooperation with Siemens was mainly oriented to the definition of a BIST and BISR scheme for memories. We published some common papers ([J4], [J1],[C1], [W2], [W1]).

8. Dissemination of knowledge and scientific excellence

8.1. Executive and organizing committees

TRUDEVICE Workshops: I organized as General Chair the first workshop for the COST Action TRUDEVICE on May 30-31, 2013 in Avignon (France) and the second on May 29-30, 2014 in Paderborn (Germany). Both workshops are held in conjunction with the European Test Symposium

European Test Symposium (ETS): I have been Publication Chair from 2012 and I will cover the role of Vice-Program Chair for ETS'15 in Cluj-Napoca (Romania)

Design, Automation and Test in Europe Conference (DATE): I cover the role of Review Chair from 2012. This role is very close to the Program Chair for the handling of the submissions, the review process, and the creation of the technical program.

Design and Test of Integrated Circuits (DTIS): I will be Vice-Program Chair for the 2014 edition in Santorini (Greece) and Program Chair in 2015 in Napoli (Italy)

VLSI Test Symposium (VTS): I have been the Publicity and Web Chair from 2006 to 2013 and Publication Chair from 2012.

Latin American Test Workshop (LATW): I cover the role of Publicity Chair from 2011.

South European Test Seminar (SETS): General Chair in 2007 and co General Chair in 2014.

8.2. Program committee and reviewer

Associate Editor of the journal: “Information Security Journal: A Global Perspective”

Guest Editor of the journal “IEEE Design & Test” for the special issue on “ETS Papers”

Guest Editor of the journal “IEEE JETTA: Journal of Electronic Testing - Theory and Applications” for the special issue on “ETS Papers”

Program Committee member:

- Design, Automation and Test in Europe Conference (DATE): from 2008 to 2011
- Latin American Test Workshop (LATW): from 2012
- VLSI Test Symposium (VTS): from 2007
- International Online Testing Symposium (IOLTS): from 2010
- European Test Symposium (ETS): from 2007
- Euromicro Conference on Digital System Design (DSD): from 2009
- Conference on Design of Circuits and Integrated Systems (DCIS): from 2006
- IEEE International Conference on Embedded and Ubiquitous Computing (EUC): from 2014
- Conference on Automation, Quality, Test and Robotics (AQTR): from 2004

Reviewer for the following Journals:

- IEEE Transaction on Computer
- IEEE Transaction on VLSI
- IEEE Design and Test of Computers

- IEEE Transactions on Emerging Topics in Computing
- IEEE Transactions on Embedded Computing Systems
- Journal of Cryptographic Engineering
- IEEE Journal of ELectronic Testing - Theory and Applications
- IEEE Transactions on Circuits and Systems
- Elsevier Microprocessors and Microsystems
- IET Computers & Digital Techniques
- International Journal of Communications, Network and System Sciences

Reviewer for the following conferences: DAC (2013), ITC (from 2008)

8.3. TTTC

The Test Technology Technical Council (TTTC) is a volunteer professional organization sponsored by the IEEE Computer Society. TTTC's goals are to contribute to our members' professional development and advancement, to help them solve engineering problems in electronic test, and to help advance the state-of-the art. In particular, TTTC aims at facilitating the knowledge flow in an integrated manner, to ensure overall quality in terms of technical excellence, fairness, openness, and equal opportunities. Since 2004 I have been strongly involved in the organization of some activities of the TTTC. In particular:

- Web Master of the "Test Technology Technical Council" (tab.computer.org/tttc) of IEEE Computer Society (from 2004)
- Vice-Chair of the Technical Activity on "HARDWARE SECURITY AND TRUST" of IEEE Computer Society TTTC (from 2011)
- TTTC Test Technology Educational Program (TTEP): Publicity Chair (from 2012)
- Chair of the Database Group of the "Test Technology Technical Council" (TTTC) of IEEE Computer Society (from 2012)
- Vice-Chair of the European "Test Technology Technical Council" (www.etttc.org) of IEEE Computer Society (2010-2013)
- Chair of the European "Test Technology Technical Council" (www.etttc.org) of IEEE Computer Society (from 2014)

8.4. GDR

Security of embedded systems is a hot topic at both French and international levels. In France, several research groups and industrial companies are extremely involved in this topic, covering multiple domains like the definition of new cryptographic algorithms, the hardware/software co-design of secure components, the study of attacks and countermeasures.

In order to allow all actors to meet and to enable knowledge exchanges in the domain of the digital hardware security, we have proposed in 2009 to create a working group in the context of the GDR SoC-SiP (*Groupe de Recherche*) owned by the CNRS. From 2009 to 2013 I covered the role of Co-Chair of the Technical Activity on "Embedded System Security”.

In this framework, we organized 7 one-day workshops on different topics:

- Hardware Security introduction: threats and countermeasures
- Side Channel Attacks
- Security of reconfigurable components
- Electro-magnetic attacks
- Cryptography and Arithmetic
- Security of Embedded Operating Systems
- PUFs and Trojans

8.5. Awards

Best paper (Transaction on Computer), awarded by a movie published at “Computing Now” (http://www.computer.org/portal/web/computingnow/1211/whatsnew/tc)

"IEEE Computer Society Golden Core Member" (2011)

"Meritorious Service Award - in recognition of more than 8 years of significant services for TTTC Electronic Media" (2007)

"Certificate of Appreciation from IEEE Computer Society for serving as TTTC Webmaster in 2006/2007" (2007)

"Certificate of Appreciation from IEEE Computer Society for serving as TTTC Webmaster in 2004/2005" (2005)

8.6. National expertises

- Review of a candidature for the ANR Young Researchers Programme (JCJC 2013)
- ANRT service CIFRE for Gemalto

Chapter III: Perspectives

My *cursus* has a clear background on all activities, disciplines and skills related to dependability, test, fault tolerance and reliability of digital systems. At the beginning of my research carrier, these skills were applied to memories and then to complex processor-based systems for which a software is running. After moving to LIRMM, I specialized in test, fault tolerance and reliability for secure devices. Moreover, I kept on working on the reliability of computer-based systems. Recently, I started analyzing the domain of the 3D stacked Integrated Circuits based on the use of Through Silicon Vias.

My perspectives are organized following the 3 main themes of my research activities: Security, Test, Dependability.

9. Perspectives on Security

Since the invention of the first integrated circuit (IC) in 1958 and introduction of first standalone Central Processing Unit (CPU) in 1971, we witnessed and continue to observe the breathtaking advances in IC manufacturing, transistor density and architectural solutions. These advances fueled the imagination of developers so that we now have diverse application fields for integrated circuits; from RF ID chips and micro-controllers to CPUs for desktop PCs with billion transistors integrated. ICs and systems have become a multibillion-dollar business and represent the physical backbone of our digitalized world. Interesting enough, they are being increasingly deployed even in many security-critical infrastructures such as sensitive governmental organizations, military, and financial/banking systems, where the impact and consequences of attacks could be catastrophic. Till recently, we have intuitively trusted the chips to control our lives and processes, so we have huge amount of sensitive information processed in chips. However, nowadays, attacks are being launched increasingly for economic reasons by well-funded criminal organizations or for intelligence purposes to get access to secret and sensitive information. Moreover, the emergence of globalized and horizontal IC and semiconductor business model, mainly driven by cost savings, is requiring both designs and users re-asses their trust in hardware and even in the supply chain. In recent years many reports have appointed to these attacks on the electronic components and their supply chain. The semiconductor industry is today loosing over $4 billion a year due to these kind of attacks; not to mention the catastrophic results these attacks could have for critical applications.

Depending on their targets, hardware attacks can be classified into three classes:

- IC data (assets) attacks: These are attacks that aim at retrieving the secret data of the IC; e.g., hacking a smart cart to get the secret key;
- IC design (IP) attacks: These are attacks that aim at getting more information on the IC design in order to counterfeit it; e.g., perform reverse engineering on an IC or IP, steal and/or even claim the ownership;
- IC functionality (tampering) attacks: these are attacks that target the alternation of the original function of the chip/system. For example, a chip ceases functioning or continues to operate but then in an impaired manner, a chip introducing corruption in the data, etc.

9.1. Asset Attacks

These types of attacks are performed in order to retrieve a secret information stored in the circuit (for instance the secret key of a circuit implementing a cryptographic algorithm). For scan-chain-based and fault attacks, the countermeasures are often based on testing and fault tolerance techniques. Based on my background, I will keep on investigating new threats and solutions for these 2 types of attacks.

9.1.1. Scan-Chain-based Attacks

Although we have proposed efficient results to counteract attacks based on the use of the scan chains, there is still room for the investigation of solutions and architecture that will allow on-site debugging facilities for the end user.

This scenario is extremely critical because, from the circuit point of view, there are no differences between an attacker or a valid user who wants to gather internal information stored within the circuit.

To address this point, I recently submitted a CHIST-ERA project to obtain enough man power to successfully solve this issue.

The main idea that it will be investigated is the re-use of the secret information within the circuit (for instance the secret encryption key) to encrypt the scan chain content. This method will deliver the content of the scan chain (i.e., the internal state of the circuit) without compromising the overall security for those users who do not know the value of the secret key. The valid user will be therefore able to decrypt the receive information, while an attacker will not be able to exploit these data.

9.1.2. Fault Attacks

The strength of the circuit against an attack is much more difficult to assess at design time w.r.t. other properties. Any vulnerabilities not detected during design phase causes the designer not only a significant economical defeat related to design time spent for useless countermeasures, but also a substantial decrease in incomes because of the non-secure product.

It is therefore essential for designers of secure devices to have a CAD environment to validate the effectiveness of their countermeasures at an early stage of the design. However, such a design environment does not currently exist in semiconductor manufacturer industry as well as in academic laboratories, especially for tomorrow's deep-submicron technologies. There are two main reasons why the task of early evaluation of a countermeasure remains still a concern. From one side, it is very difficult to understand and to model physical phenomena underlying a fault attack, especially for new technologies. On the other hand, there are no available CAD tools that incorporate such models to simulate the effect of an injection. In the project we will focus on laser injections because this type of attack has been proved to be extremely effective.

In the future year, thanks to the cooperations with the ONERA and the Ecole de Mines (Gardanne), in the conext of the LIESSE project we will try to measure and characterize the real effect of laser shots onto deep submicron circuits.

Starting from these physical observations, we will try to create electrical- and gate-level models of the laser shots onto the circuit, in order to deliver CAD tools for simulation and/or emulation of laser induced effects. This type of tool will allow efficiently validating possible countermeasures that will be proposed in the future.

The reason of this research direction resides on several aspects. First, no electrical models of laser shots onto the circuit exist yet. It is possible to find several models for older technologies, while the effect of laser injections on 65nm (and beyond) circuit technology still remain an open issue. Second, the integration of the strength analysis for a countermeasure in CAD tools is not mature yet. The common industry practice is to validate the efficiency of a countermeasure after the production of the device, by physically attacking the circuit. Possibly, for applications that require a high level of security, the circuit can be instrumented with light sensors raising an alert whenever a laser attack is performed. However this type of solution is extremely expensive. The solution we will propose will allow the designer to implement cheaper countermeasures without compromising the overall circuit security.

9.2. IP Attacks

Fabless semiconductor industries are facing new threats, i.e., the possibility for the manufacturer to re-use the masks for producing additional copies (clones). The cloned ICs are built in the same or similar factories as the original and legal ones, and then sold within illegal markets. IC cloning must be prevented for several reasons: 1. the risk for future customers to rely on non-reliable products since clones are not fully characterized and tested by the company that designed the IC, 2. the economic loss that follow on from the first risk, since non-reliable products stamped with the fabless company name have a disastrous effect on the public image of the company, 3. the obvious additional economic losses for the fabless company that does not profit from the illegal market.

We recently studied a possible solution to prevent integrated circuits from being cloned, by covering the whole production chain (from the design of reliable embedded anti-cloning structures to the secured activation of the legal ICs using dedicated production tests). An important aspect of the proposed approach is the emphasis given to cost issues, which is a true novelty. Indeed, industrials are facing with two choices so far: either a very sophisticated and efficient protection, which are thus relatively expensive and consequently applied in very specific markets like identification, or no protection at all. We intend to bridge the gap and propose an affordable solution that will raise the cost of counterfeiting to the minimum level that makes it pointless.

The main objective is to propose and validate an overall scheme to protect standard CMOS integrated circuits from being copied by optical cloning using one of these means: mask theft or basic reverse engineering. This scheme must be easy to implement, transparent from the customer point of view and with negligible impact on the die cost. This will imply the development of digital IPs along with a process of authentication to be run during industrialization. For that latter, emphasis is put on the seamless integration of the activation phase during the latest steps of industrialization.

9.3. Tampering Attacks

The cost of new fabrication facilities is becoming more and more prohibitive and outsourcing the fabrication process to low-cost locations has become a major trend in Integrated Circuit (IC) industry in the last decade. Untrusted foundries may therefore manipulate the circuits with the possible insertion of Hardware Trojan Horses (HTs) are malicious alterations of integrated circuits (ICs) introduced at design or fabrication steps in order to modify the circuit's intended behavior when deployed in the field. The goal of such alterations can be to introduce a hidden functionality, reduce the IC's reliability, let leak sensitive information or cause a denial of service. HTs can be designed to be always on, i.e. able to affect the infected circuit at any time, or they may require an internal or external trigger to become active.

Due to the diversity of possible implementations, activation and effects on the IC's functionality, the detection of HTs is a very challenging task. Recently, numerous detection approaches have been published for post-silicon trust validation. Most of them assume that the design, layout and testing steps are trusted, while the fabrication facility is the only untrusted step of the design flow. HT detection approaches can be destructive or not; for the latter ones, detection mechanisms can be applied at test time or run-time. Non-destructive methods are divided into two categories: side-channel analysis and logic testing. I will focus on techniques based on logic testing, in which the principle is to stimulate the input ports of an IC and monitor its outputs. If an erroneous behavior of the IC is observed, it can be inferred that a HT has been inserted in the IC. However, traditional ATPG testing may not be sufficient to detect HTs which are indeed stealthy in nature i.e. mostly inactive unless they are triggered by a "rare value". The main goal is therefore to be able to activate potential HTs. We started investigating a procedure to identify circuit sites where a possible HT may easily be inserted. The selection of the sites is based on the following assumptions:

- a potential HT is triggered by nodes with a rare value (i.e. that are very rarely '0' or very rarely '1)
- the trigger is inserted in paths that are not critical in terms of delay
- the trigger will be composed of multiple gates that are close one to the other in the circuit's layout, and close to available space.

This activity is in the preliminary phase and it will be developed in-depth.

10. Perspectives on Test

3-Dimensional (3D) integration is an emerging technology where multiple layers of planar 2D devices (tiers) are stacked and interconnected using so called Through Silicon Vias (TSVs). Besides footprint advantages, the potential benefits of 3D integration can include higher device speed, smaller overall cost, lower power consumption, larger bandwidth, and it will allows heterogeneous designs. Unfortunately, die stacking also presents new challenges. Among them, test and testability must be redefined for 3D.

In particular, the test strategy must be specifically defined to cope with this fabrication process. When test steps are expected at different level of the stacking process (pre-bond, mid-bond, and post-bond testing), they should be enabled by the same test infrastructure for cost reduction. Moreover, introduction of TSVs for inter-die interconnection requires specific test steps for these elements. Test wrappers must also be defined for isolation and test access to the different dies.

In 2011, we started a new research axis, in collaboration with CEA Leti, continuing within the framework of the european project MASTER3D for the definition of a complete 3D Design for Testability approach. Assuming that the 3D circuit can be accessed only from the bottom (bottom layer), additional TSVs are needed to drive test data from the bottom die to upper dies, and boundary scan cells are used to form a die level wrapper either based on IEEE 1500 or IEEE 1149.1 standards.

We are currently studying the existing test standards (IEEE 1149.1, IEEE 1500, IEEE 1149.7, and P1687) showing advantages and drawbacks of each one for 3D circuits. We want to propose custom and dedicated extensions for coping with pre-bond testing of TSVs, post-bond testing of TSVs and obtained stack.

We are currently developing such infrastructures with related test-scheduling strategies by using the P1687 IJTAG standard. This architecture relies on the usage of automatic die detectors, and it allows pre-, mid- and post- bond testing. The reason why we selected the P1687 standard is that it easily allows the retargeting of test patterns.

Our future works will deal with the test scheduling taking into account not only test bandwidth but also power and thermal issues which are specific to 3D circuits. The scheduling method will also consider the manufacturing step in which the circuit is being tested (partial or final stack).

11. Perspectives on Dependability

Information technology is at the core of our society and it relies completely on the design of electronic information processing systems. Today's computing is a true continuum that ranges from smart-phones to mission-critical datacenter machines, and from desktops to automobiles. On aggregate, these computing devices represent a total addressable market approaching a billion processors a year, which is expected to explode to more than two billion per year before 2020.

The computing industry move towards the "computing continuum" means that the same key technologies and industrial players will act across all computing segments: airplanes, automobile, buildings, health instruments, smart-phones, tablets, desktops, servers, data-centers, clouds, high-performance computing (HPC), etc. Therefore, in the near future we will see embedded systems (ES) with HPC performance and functionalities, HPC systems used in time- and safety-critical applications, cloud resources used with very different business models, etc.

For more than three decades, industry has evolved by roughly doubling the device density (and corresponding performance) every two years following Moore's law. However, future device integration technology is expected to dramatically reduce the device quality, and therefore the operational reliability of circuits: as the transistors and wires shrink, they show both larger differences in behavior although they are designed to be identical (device variability, manufacturing defects, aging), and higher susceptibility to transient and permanent faults (soft-errors, wear-out). The great challenge for future technologies is building "dependable" systems on top of unreliable components, which will degrade and even fail during normal lifetime of the chip.

Conventional design techniques expend significant amount of energy to tolerate the device unpredictability by adding safety margins to a circuit's operating voltage, clock frequency or charge stored per bit. However, the rising energy costs needed to compensate for increasing unpredictability are rapidly becoming unacceptable in today's environment where power consumption is often the limiting factor on integrated circuit performance, and energy efficiency is a top concern. Implementing the computing continuum in this era, where low reliability threatens to end the benefits of feature size reduction, requires a holistic approach across different computing disciplines, across computing system layers and across computing market segments to have a unique reliability assessment methodology.

In the next years, and thanks to the CLERECO project, I want to investigate the problem of having an early, fast, and accurate evaluation of computing systems reliability to support design decisions for hardware and software reliability enhancing mechanisms in the system. Such a framework will be a key enabler for the continuation of technology scaling benefits harnessing for several decades. Moreover, it will also enable the implementation of the computing continuum that societal services demand.

The benefits of an early and accurate methodology for the computing continuum to estimate the reliability are many. First, a tool that yields early estimate allows designers to reduce the time-to-market (TTM) of all products, enabling the fast turnaround of proliferation of computing systems tailored to customers' needs. Second, accurate reliability estimates allow developing the required cost- and energy- efficient reliability solutions at the hardware and software layers. Such solutions can be only developed if the expected reliability of the system can be quickly and accurately assessed: (a) at different stages of the design flow (from design concept and early design stages through first silicon validation and eventually during operation in the field), (b) considering the impact of all hardware and software components, and the different modes of operation (use cases) of the system. Finally, the development of a reliable and dependable product that employs mechanisms to detect and handle possible faults can reduce the overall life cycle costs.

Chapter IV: Publications

12. Book chapters

[B2] K. Bousselam, G. Di Natale, M.-L. Flottes, B. Rouzeyre
On Countermeasures Against Fault Attacks on Advanced Encryption Standard,
"Fault Analysis in Cryptography", in the series "Springer-Verlag's Information Security and Cryptography", 2012

[B1] K. Bousselam, G. Di Natale, M.-L. Flottes and B. Rouzeyre
Fault Detection in Crypto-Devices,
In book "Fault Detection", Wei Zhang (Ed.), ISBN: 978-953-307-037-7, InTech, March 2010

13. Journals

[J18] Amitabh Das, Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, Ingrid Verbauwhede
Test versus Security: Past and Present,
IEEE Transactions on Emerging Topics in Computing, DoI: 10.1109/TETC.2014.2304492, February 2014

[J17] Jean-Max Dutertre, Rodrigo Possamai Bastos, Olivier Potin, Marie-Lise Flottes, Bruno Rouzeyre and Giorgio Di Natale
Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection,
Microelectronics Reliability (Elsevier), Volume 53, Issues 9-11, September-November 2013, Pages 1320-1324, DOI: 10.1016/j.microrel.2013.07.069

[J16] Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
Thwarting Scan-Based Attacks on Secure-ICs with On-Chip Comparison,
IEEE Transaction on VLSI, DOI: 10.1109/TVLSI.2013.2257903

[J15] Amitabh Das, Jean Da Rolt, Santosh Ghosh, Stefaan Seys, Sophie Dupuis, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, Ingrid Verbauwhede
Secure JTAG Implementation Using Schnorr Protocol,
Journal of Electronic Testing (JETTA), Springer, DOI: 10.1007/s10836-013-5369-9

[J14] R. Possamai Bastos, G. Di Natale, M. Flottes, F. Lu, B. Rouzeyre
A New Recovery Scheme against Short-to-Long Duration Transient Faults in Combinational Logic,
Journal of Electronic Testing (JETTA), Springer, DOI: 10.1007/s10836-013-5359-y

[J13] Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
A Novel Differential Scan Attack on Advanced DFT Structures,
ACM Transactions on Design Automation of Electronic Systems, Vol. 18, Is. 4, Oct. 2013, Article No. 58, DOI: 10.1145/2505014

[J12] Jean Da Rolt, Amitabh Das, Santosh Ghosh, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre and Ingrid Verbauwhede
Scan Attacks on Side-channel and Fault Attack Resistant Public-key Implementations,
Journal of Cryptographic Engineering, November 2012, Volume 2, Issue 4, pp 207-219, DOI: 10.1007/s13389-012-0045-z

[J11] R. Possamai Bastos, F. Sill Torres, G. Di Natale, M. Flottes, B. Rouzeyre
Novel Transient-Fault Detection Circuit Featuring Enhanced Bulk Built-in Current Sensor with Low-Power Sleep Mode,
Microelectronics Reliability (Elsevier), Volume 52, Issues 9-10, September-October 2012, Pages 1781-1786, DOI: 10.1016/j.microrel.2012.06.149

[J10] A. Savino, S. Di Carlo, G. Politano, A. Benso, A. Bosio, G. Di Natale
Statistical reliability estimation of microprocessor-based systems,
IEEE Transaction on Computer, Volume PP, Issue 99, October 2011, DOI: 10.1109/TC.2011.188

[J9] G. Di Natale, M. Doulcier, M. L. Flottes, B. Rouzeyre
Self-Test Techniques for Crypto-Devices,
IEEE Transaction on VLSI Systems, pp. 1-5, 2009, DOI: 10.1109/TVLSI.2008.2010045

[J8] G. Di Natale, M. Doulcier, M. L. Flottes, B. Rouzeyre
A Reliable Architecture for Parallel Implementations of the Advanced Encryption Standard,
Journal of Electronic Testing (JETTA), Springer, Volume 25 Issue 4-5, August 2009, pp. 269-278, DOI: 10.1007/s10836-009-5106-6

[J7] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
March Test Generation Revealed,
IEEE Transaction on Computer, Volume 57, Issue 12, Dec. 2008 Page(s):1704 - 1713, DOI: 10.1109/TC.2008.105

[J6] A. Bosio, G. Di Natale
March Test BDN: A new March Test for Dynamic Faults,
Journal of Control Engineering and Applied Informatics (CEAI), Nr.2, Volume 10, June 2008, pp. 3-9

[J5] A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
March AB, a State-of-the-Art March Test for Realistic Static Linked Faults and Dynamic Faults in SRAMs,
IEE Proceedings Computers and Digital Techniques, Vol. 1, No. 3, May 2007, pp. 237-245

[J4] A. Benso, S. Di Carlo, G. Di Natale, M. Lobetti Bodoni, P. Prinetto,

Programmable Built-In Self-Testing of Embedded RAM Clusters in System-on-Chip Architectures,
IEEE Communications Magazine, Vol. 41, N. 9, September 2003, pp. 90-97

[J3] A. Benso, S. Di Carlo, G. Di Natale, J.F. Panico, P. Prinetto,
On-Line Self-Repair of Finite Impulse Response Filters,
IEEE Design and Test of Computers, May-June 2003, pp. 50-57

[J2] A. Benso, S. Chiusano, G. Di Natale, P. Prinetto,
An On-line BISTed RAM Architecture with Self Repair Capabilities,
IEEE Transaction on Reliability, Vol. 51 Issue. 1, Mar 2002, pp. 123, 128

[J1] A. Benso, S. Chiusano, G. Di Natale, M. Lobetti-Bodoni, P. Prinetto,
On-line & Off-line BIST in IP-Core Design,
IEEE Design and Test of Computers, September/October 2001, Vol. 18, N. 5, pp. 92-99

14. Conferences, Symposium, Workshops, Presentations

References listed below have been numbered by using a letter before the number of the reference. The meaning of the letter is the following:

- C = Conference with official proceedings and review process
- S = Symposium with official proceedings and review process
- W = Workshop with official proceedings and review process
- P = presentation (in a conference, symposium or workshop) without official proceedings.

[C14] Giorgio Di Natale, Marie-lise Flottes, Bruno Rouzeyre, Hakim Zimouche
Built-In Self-Test for Manufacturing TSV Defects before bonding,
IEEE VLSI Test Symposium 2014 (VTS'14)

[S30] Hakim Zimouche, Giorgio Di Natale, Marie-lise Flottes, Bruno Rouzeyre
A BIST Method for TSVs Pre-Bond Test,
8th IEEE International Design and Test Symposium (IDT13), Marrakesh (Morocco), 16-18 December 2013

[P35] Jean-Max Dutertre, Rodrigo Possamai Bastos, Olivier Potin, Marie-Lise Flottes, Bruno Rouzeyre and Giorgio Di Natale
Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection,
24th European Symposium on Reliability of Electron Devices, Failure Physics and Analysis (ESREF'13)

[P34] Yassine Fkih, Pascal Vivet, Bruno Rouzeyre, Marie-lise Flottes, Giorgio Di Natale, Juergen Schloeffel
3D Design For Test Architectures Based on IEEE P1687,
3D-Test: Fourth IEEE International Workshop on Testing Three-Dimensional Stacked Integrated Circuits

[P33] Jean-Max Dutertre, Rodrigo Possamai Bastos, Olivier Potin, Marie-Lise Flottes, Bruno Rouzeyre and Giorgio Di Natale
Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection,
24th European Symposium on Reliability of Electron Devices, Failure Physics and Analysis (ESREF'13)

[W18] Rodrigo Possamai Bastos, Frank Sill Torres, Jean-Max Dutertre, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre
A Single Built-in Sensor to Check Pull-up and Pull-down CMOS Networks against Transient Faults,
23th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS'13)

[C13] Feng Lu, Giorgio Di Natale, Marie-Lise Flottes and Bruno Rouzeyre
Laser-Induced Fault Simulation,
16th Euromicro Conference on Digital System Design (DSD 2013), Spain, 4-6 September, 2013

[S29] J.Da Rolt, G.Di Natale, M.-L.Flottes, B.Rouzeyre
A Smart Test Controller for Scan Chains in Secure Circuits,
IEEE International On-Line Testing Symposium 2013 (IOLTS,13), July 2013

[W17] F. Lu, G. Di Natale, M. Flottes, B. Rouzeyre
tLIFTING: an Open-Source Multi-Level Fault Simulator for Ionizing Effects,
9th Conference on Ph. D. Research in Microelectronics and Electronics, Villach, Austria, June 24th-27th, 2013 - SILVER LEAF Certificate

[W16] Y. Fkih, P. Vivet, B. Rouzeyre, M. Flottes, G. Di Natale
A JTAG Based 3D DfT Architecture Using Automatic Die Detection,
9th Conference on Ph. D. Research in Microelectronics and Electronics, Villach, Austria, June 24th-27th, 2013 - BRONZE LEAF Certificate

[P32] F. Lu, G. Di Natale, M.-L. Flottes, B. Rouzeyre
A multi-level simulation tool for laser attacks,
CryptArchi'13: Cryptographic Architectures Embedded in Reconfigurable Devices, France (2013)

[P31] Giorgio Di Natale
Manufacturing Test of 3D Stacked ICs: Problems, Solutions and Standards,
Design for 3D Workshop, June 26-28 2013, Grenoble (France)

[C12] Yassine Fkih, Pascal Vivet, Bruno Rouzeyre, Marie-Lise Flottes, Giorgio Di Natale
A 3D IC BIST for Pre-Bond Test of TSVs Using Ring Oscillators,
NEWCAS 2013, 11th IEEE INTERNATIONAL NEWCAS CONFERENCE, France (2013)

[S28] Rodrigo Possamai Bastos, Frank Sill Torres, Jean-Max Dutertre, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre
A Bulk Built-in Sensor for Detection of Fault Attacks,
IEEE International Symposium on HARDWARE-ORIENTED SECURITY and TRUST (HOST'13)

[P30] F. Lu, G. Di Natale, M.-L. Flottes, B. Rouzeyre
Laser-Induced Fault Simulation,
1st TRUDEVICE Workshop, May 30-31, Avignon (France)

[P29] G. Di Natale, S. Dupuis, M.-L. Flottes, B. Rouzeyre
Identification of Hardware Trojan's Triggering Signals,
1st TRUDEVICE Workshop, May 30-31, Avignon (France)

[P28] Giorgio Di Natale
TRUDEVICE: A COST Action on "Trustworthy Manufacturing and Utilization of Secure Devices",
IEEE European Test Symposium (ETS'13), May 27-30 2013, Avignon (France)

[P27] G. Di Natale, M.-L. Flottes, F. Lu, B. Rouzeyre
tLIFTING: an Open-Source Delay-Annotated Fault Simulator,
XXVII Conference on Design of Circuits and Integrated Systems (DCIS'2012), Avignon (F), November 2012

[P26] G. Di Natale, S. Dupuis, B. Rouzeyre
Is Side-Channel Analysis really reliable for detecting Hardware Trojans?,
XXVII Conference on Design of Circuits and Integrated Systems (DCIS'2012), Avignon (F), November 2012

[P25] J. Da Rolt, G. Di Natale, M.-L. Flottes, B. Rouzeyre
On-chip test comparison for protecting confidential data in secure ICs,
XXVII Conference on Design of Circuits and Integrated Systems (DCIS'2012), Avignon (F), November 2012

[W15] J. Darolt, A. Das, G. Di Natale, M.-L. Flottes, B. Rouzeyre, I. Verbauwhede
A New Scan Attack on RSA in Presence of Industrial Countermeasures,
Third International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE'12), Lecture Notes in Computer Science Volume 7275, pp. 89-104

[S27] J. Darolt, A. Das, G. Di Natale, M.-L. Flottes, B. Rouzeyre, I. Verbauwhede
A New Scan Attack on Elliptic Curve Cryptosystems in presence of Industrial Design for Testability Structures,
IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT'12)

[P24] Rodrigo Possamai Bastos, F. Sill Torres, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
Novel transient-fault detection circuit featuring enhanced bulk built-in current sensor with low-power sleep-mode,
23th European Symposium on Reliability of Electron Devices, Failure Physics and Analysis (ESREF'12)

[S26] J. Darolt, G. Di Natale, M-L. Flottes, B. Rouzeyre
On-chip test comparison for protecting confidential data in secure ICs,
IEEE European Test Symposium 2012 (ETS'12), DOI: 10.1109/ETS.2012.6233039

[S25] J. Darolt, G. Di Natale, M-L. Flottes, B. Rouzeyre
Are advanced DfT structures sufficient for preventing scan-attacks,
IEEE VLSI Test Symposium 2012 (VTS'12), pp. 246-251, DOI: 10.1109/VTS.2012.6231061

[P23] G. Di Natale, M. L. Flottes, R. Giroudeau, F. Hernandez
Exact Wafer Matching Process for 3D Wafer-to-Wafer Integration,
3D Integration: Applications, Technology, Architecture, Design, Automation, and Test Workshop (poster)

[S24] R. Possamai Bastos, G. Di Natale, M-L. Flottes, B. Rouzeyre
A New Bulk Built-In Current Sensor-Based Strategy for Dealing with Long-Duration Transient Faults in Deep-Submicron Technologies,
IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, Vancouver (Canada), 3-5 Oct. 2011, pp.302-308, DOI: 10.1109/DFT.2011.15

[C11] R. Possamai Bastos, G. Di Natale, M-L. Flottes, B. Rouzeyre
How to Sample Results of Concurrent Error Detection Schemes in Transient Fault Scenarios?,
RADECS'2011: Conference on Radiation Effects on Components and Systems, Sevilla (Spain), pp. 635-642, DOI: 10.1109/RADECS.2011.6131361

[P22] J. Darolt, G. Di Natale, M-L. Flottes, B. Rouzeyre
New side-channel attack against scan chains,
CryptArchi'11: Cryptographic Architectures Embedded in Reconfigurable Devices, Germany (2011)

[S23] J. Darolt, G. Di Natale, M.L. Flottes, B. Rouzeyre
New security threats against chips containing scan chain structures,
IEEE International Symposium on Hardware-Oriented Security and Trust 2011 (HOST'11), June 2011 (San Diego, CA, USA), pp. 105-110, DOI: 10.1109/HST.2011.5955005

[S22] J. Darolt, G. Di Natale, M.L. Flottes, B. Rouzeyre
Scan attacks and countermeasures in presence of scan response compactors,
IEEE European Test Symposium 2011 (ETS'11), May 2011 (Trondheim, Norwey), pp. 19-24, DOI: 10.1109/ETS.2011.30

[W14] G. Di Natale, M.L. Flottes, B. Rouzeyre, D. Real
Power Consumption Traces Realignment to Improve Differential Power Analysis,
IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS'11), April 2010, Cottbus (Germany)

[W13] R. Possamai Bastos, G. Di Natale, M-L. Flottes, B. Rouzeyre
Timing issues for an efficient use of concurrent error detection codes,
IEEE Latin American Test Workshop 2011 (LATW'11), pp. 1-6, DOI: 10.1109/LATW.2011.5985933

[P21] A. Bosio, G. Di Natale
Parallel Test of Identical Cores using Test Elevators in 3D circuits extended abstract,
IEEE International Workshop on Testing Three-Dimensional Stacked Integrated Circuits (3D-TEST'10), Austin (Texas), October 2010

[S21] K. Bousselam, G. Di Natale, M.L. Flottes, B. Rouzeyre
Evaluation of Concurrent error detection techniques on the Advanced Encryption Standard,
IEEE International On-Line Testing Symposium 2010 (IOLTS,10), July 2010, Corfu, pp. 223-228

[P20] G. Di Natale, M-L. Flottes, B. Rouzeyre
Waveforms re-alignment to improve DPA attacks,
CryptArchi'10: Cryptographic Architectures Embedded in Reconfigurable Devices, France (2010)

[S20] K. Bousselam, G. Di Natale, M.L. Flottes, B. Rouzeyre
Evaluation of Concurrent error detection techniques on the Advanced Encryption Standard,
IEEE European Test Symposium 2010 (ETS'10), May 2010 (Praha), pp. 252-252 (Poster)

[P19] G. Di Natale, B. Rouzeyre
Embedded Tutorial on "Test and Security",
Presented to IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS'10), April 2010, Vienna (Austria)

[S19] G. Di Natale, M.L. Flottes, B. Rouzeyre
Evaluation of Resistance to Differential Power Analysis: Execution Time Optimizations for Designers,
IEEE International Symposium on Electronic Design, Test & Applications (DELTA 2010), Vietnam (Ho Chi Minh City), January 2010, pp. 256-261

[P18] Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
An Integrated Validation Environment for Differential Power Analysis,
DATE 2010, University Booth

[P17] Alberto Bosio, Giorgio Di Natale
LIFTING: an Open-Source Logic Simulator,
DATE 2010, University Booth

[P16] G. Di Natale, M.L. Flottes, P. Maistri
Embedded Tutorial on "Test and Security",
Presented to IEEE European Test Symposium 2009 (ETS'09)

[W12] G. Di Natale, M. L. Flottes, B. Rouzeyre
Execution Time Reduction of Differential Power Analysis Experiments,
IEEE Latin American Test Workshop 2009 (LATW'09)

[P15] G. Di Natale, M.L. Flottes
Embedded Tutorial on "Test and Security",
Presented to IEEE Latin American Test Workshop 2009 (LATW'09)

[S18] Stefano Di Carlo, Giorgio Di Natale, Riccardo Mariani
On-Line Instruction-checking in Pipelined Microprocessors,
IEEE International Asian Test Symposium (ATS 2008), 2008

[S17] Alberto Bosio, Giorgio Di Natale
LIFTING: a Flexible Open-Source Fault Simulator,
IEEE International Asian Test Symposium (ATS 2008), 2008

[P14] G. Di Natale, M. L. Flottes, B. Rouzeyre
A Reliable Architecture for Substitution Boxes in Integrated Cryptographic,
International Conference on Design of Circuits and Integrated Systems, Grenoble, 2008

[P13] Alberto Bosio, Giorgio Di Natale
LIFTING: an Open-Source Logic Simulator,
SAME (Sophia Antipolis Micro Electronics) 2008 Forum

[P12] Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
An Integrated Validation Environment for Differential Power Analysis,
SAME (Sophia Antipolis Micro Electronics) 2008 Forum

[P11] Philipp Öhler, Sybille Hellebrand, Alberto Bosio, Giorgio Di Natale
Modularer Selbsttest und optimierte Reparaturanalyse für eingebettete Speicher,
Zuverlässigkeit und Entwurf, September 2008, pp. 49-56

[S16] Philipp Öhler, Alberto Bosio, Giorgio Di Natale, Sybille Hellebrand
A Modular Memory BIST for Optimized Memory Repair,
IEEE International On-Line Testing Symposium (IOLTS 2008), July 2008, pp. 171-172

[P10] Di Natale G., Flottes M-L, Rouzeyre B.
An Integrated Validation Environment for Differential Power Analysis,
CryptArchi'08: Cryptographic Architectures Embedded in Reconfigurable Devices, France (2008)

[P9] G. Di Natale, M. L. Flottes, B. Rouzeyre
Stuck-at-Faults Test using Differential Power Analysis,
Low Power design on Test & Reliability Workshop (LPonTR 2008)

[C10] A. Bosio, G. Di Natale
March Test BDN: A new March Test for Dynamic Faults,
IEEE International Conference on Automation, Quality & Testing, Robotics (AQTR'08), May 2008, pp. 85-89

[S15] G. Di Natale, M. Doulcier, M.-L. Flottes, B. Rouzeyre
A Reliable Architecture for the Advanced Encryption Standard,
IEEE European Test Symposium 2008 (ETS'08), May 2008, pp. 13-18

[P8] G. Di Natale, M. Doulcier, M. L. Flottes, B. Rouzeyre
Low-Cost Self-Test of Crypto Devices,
Workshop on Dependable and Secure Nanocomputing (wDSN 2008)

[W11] G. Di Natale, M.-L. Flottes, B. Rouzeyre
Observability of Stuck-at-Faults with Differential Power Analysis,
IEEE Latin-American Test Workshop (LATW 2008), Puebla (Mexico), February 2008

[S14] G. Di Natale, M.-L. Flottes, B. Rouzeyre
An Integrated Validation Environment for Differential Power Analysis,
IEEE International Symposium on Electronic Design, Test & Applications (DELTA 2008), Hong Kong, January 2008, pp. 527-532

[S13] M. Hosseinabady, M. H. Neishaburi, Zainalabedin Navabi, Alfredo Benso, Stefano Di Carlo, Paolo Prinetto, Giorgio Di Natale
Analysis of System-Failure Rate Caused by Soft-Errors using a UML-Based Systematic Methodology in an SoC,
IEEE International On-Line Testing Symposium (IOLTS 2007), Heraklion (Crete, Greece), July 2007, pp. 205-206

[S12] Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
An On-Line Fault Detection Scheme for SBoxes in Secure Circuits,
IEEE International On-Line Testing Symposium (IOLTS 2007), Heraklion (Crete, Greece), July 2007, pp. 57-62

[P7] Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
A Dependable Parallel Architecture for SBoxes,
Reconfigurable Communication-Centric SoCs (ReCoSoc 2007), Montpellier : France (2007)

[P6] Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
On-Line Self-Test of AES Hardware Implementations,
Workshop on Dependable and Secure Nanocomputing (DSN 2007), Edinburgh (UK)

[P5] Flottes M-L, Di Natale G., Rouzeyre B., Doulcier M.
Test and Security,
CryptArchi'07: Cryptographic Architectures Embedded in Reconfigurable Devices, France (2007)

[W10] Di Natale G., Flottes M.-L., Rouzeyre B.
A Novel Parity Bit Scheme for SBOX in AES Circuits,
IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS'07), April 2007, pp. 267-271

[S11] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
Memory Fault Simulator for Static-Linked Faults,
IEEE Asian Test Symposium (ATS 2006), Fukuoka (J), November 2006

[S10] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
ATPG For Dynamic Burn-In Test in Full-Scan Circuits,
IEEE Asian Test Symposium (ATS 2006), Fukuoka (J), November 2006

[P4] M. Fischerova, T. Pikula, M. Simlastik, A. Bosio, S. Di Carlo, G. Di Natale
A tool for teaching memory testing based on BIST,
Baltic Electronics Conference, 2006 International, Oct. 2006, pp. 1-4

[P3] A. Bosio, S. Di Carlo, G. Di Natale, M. Fischerova, T. Pikula, M. Simlastik
Interactive Educational Tool for Memory Testing,
6th European Workshop on Microelectronics Education (EWME'06), Stockholm (Sweden), June 2006

[S9] M. Hosseinabady, P. Lotfi-Kamran, G. Di Natale, S. Di Carlo, A. Benso, P. Prinetto
Single-Event Upset Analysis and Protection in High Speed Circuits,
IEEE European Test Symposium 2006 (ETS'06), May 2006, pp. 29-34

[S8] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
22n March Test for Realistic Static Linked Faults in SRAMs,
IEEE European Test Symposium 2006 (ETS'06), May 2006, pp. 49-54

[C9] G. Di Natale, A. Serra, C. Turcotti
A board implementation for Fast APA Acoustic Echo Canceller using ADSP-21065L DSP,
IEEE International Conference on Automation, Quality & Testing, Robotics (AQTR'06), May 2006

[C8] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
Automatic March Tests Generations for Static Linked Faults in SRAMs,
IEEE Design Automation and Test Conference in Europe (DATE 2006), Munich (D), March 2006, pp. 1-6

[W9] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
A Unique March Test Algorithm for the Wide Spread of Realistic Memory Faults in SRAMs,
IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS'06), April 2006, pp. 155-156

[W8] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
Automatic March Tests Generation for Multi-Port SRAMs,
IEEE International Workshop on Electronic Design, Test & Applications (DELTA 2006), January 2006

[C7] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto,
March AB, March AB1: New March Tests for Unlinked Dynamic Memory Faults,
IEEE International test Conference, Austin (Texas, USA), October 2005

[P2] T. Pikula, G. Di Natale, E. Gramatová,
Built-in Self-Test Generation for Delay Faults - a case study,
5th Electronic Circuits and Systems Conference (ECS'05), September 8-9, 2005, Bratislava (Slovak Republic)

[S7] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto,
Automatic March Tests Generation for Static and Dynamic Faults in SRAMs,
IEEE European Test Symposium, 2005, May 22-25 2005, pp. 122-127

[W7] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto, L. Tagliaferri, C. Tibaldi,
PROMON: A Profile Monitor of Software Applications,
8th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS'05), April 13-16 2005, pp. 81-86

[W6] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto,
AFSM-Based Deterministic Hardware TPG,
8th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS'05), April 13-16 2005, pp. 178-181

[S6] F. Bertuccelli, F. Bigongiari, A. Brogna, G. Di Natale, P. Prinetto, R. Saletti,
Exhaustive test of several dependable memory architectures designed by GRAAL tool,
IEEE 12th Asian Test Symposium, Nov. 2003, pp. 32-35

[C6] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto, L. Tagliaferri,
Data Criticality Estimation in Software Applications,
IEEE International Test Conference, Charlotte (NC), October 2003, pp. 802-810

[S5] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto,
A Watchdog Processor to Detect Data and Control Flow Errors,
IEEE On-line Test Symposium, Kos (GR), July 2003, pp. 144-148

[S4] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto, I. Solcia, L. Tagliaferri,
FAUST: FAUlt-injection Script-based Tool,
IEEE On-line Test Symposium, Kos (GR), July 2003, p. 160

[W5] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto, L. Tagliaferri,
Data Criticality Estimation in Software Applications,
IEEE European Test Workshop, May 2003, Maastricht (NL), pp. 231-236

[S3] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto,
Specification and Design of a new Memory Fault Simulator,
IEEE Asian Test Symposium (ATS 2002), November 2002, pp. 92-97

[C5] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto,
Static Analysis of SEU Effects on Software Applications,
IEEE International test Conference, Baltimore (Maryland), October 2002, pp. 500-508

[C4] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto,
An Optimal Algorithm for the Automatic Generation of March Tests,
IEEE Design Automation and Test Conference in Europe (DATE 2002), Paris (F), February 2002, pp. 938-943

[S2] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto, L. Tagliaferri,
Control-Flow Checking Via Regular Expressions,
IEEE Asian Test Symposium (ATS 2001), Kyoto (J), November 2001, pp. 299-303

[S1] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto,
Memory Read Faults: Taxonomy and Automatic Test Generation,
IEEE Asian Test Symposium (ATS 2001), Kyoto (J), November 2001, pp. 157-163

[C3] G. Di Natale, S. Chiusano, P. Prinetto, F. Bigongiari,
GRAAL: a Tool for Highly Dependable SRAMs Generation,
IEEE International Test Conference (ITC01), USA, October 2001

[W4] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto, L. Tagliaferri,
Software Dependability Techniques validated via Fault Injection Experiments,
Proc. RADECS 2001, Grenoble (F), September 2001, pp. 269-274

[W3] A. Benso, S. Di Carlo, G. Di Natale, L. Tagliaferri, P. Prinetto,
Validation of a Software Dependability Tool via Fault Injection Experiments,
IEEE International On-Line Test Workshop (IOLTW 2001), Italy, July 2001, pp. 3-8

[C2] A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto,
SEU Effect Analysis in Open-Source Router via a Distributed Fault Injection Environment,
IEEE Design Automation and Test Conference in Europe (DATE 2001), Munich (D), February 2001, pp. 219-223

[P1] A. Benso, R. Mariani, G. Di Natale, P. Prinetto,
On Evaluating DSP-based Architectures for Space Application,
XV Conference on Design of Circuits and Integrated Systems (DCIS'2000), Montpellier (F), November 2000, pp. 421-426

[C1] A. Benso, S. Di Carlo, G. Di Natale, M. Lobetti-Bodoni, P. Prinetto,
A programmable BIST architecture for clusters of Multiple-Port SRAMs,
IEEE International Test Conference (ITC00), Atlantic City (NJ), USA, October 2000, pp. 557-566

[W2] A. Benso, S. Chiusano, G. Di Natale, M. Lobetti-Bodoni, P. Prinetto,
A family of Self-Repair SRAM cores,
International On-Line Test Workshop (IOLTW00), Majorca (ES), July 2000, pp. 214-218

[W1] A. Benso, S. Chiusano, S. Di Carlo, G. Di Natale, P. Prinetto, M. Lobetti-Bodoni,
An effective distributed BIST architecture for RAMs,
IEEE European Test Workshop (ETW00), Lisbon (P), May 2000, pp. 119-124

15. Patent

Reference code (French coding): 13 52306

Title: “Procédé, dispositif et système de détection automatique de défauts ns des vias TSV”

Inventors: Pascal VIVET, Giorgio DI NATALE; Yassine FKIH, Marie)-Lise FLOTTES, Bruno ROUZEYRE

Chapter V: Selection of 5 best papers

[J16] Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
Thwarting Scan-Based Attacks on Secure-ICs with On-Chip Comparison,
IEEE Transaction on VLSI, DOI: 10.1109/TVLSI.2013.2257903

[J14] R. Possamai Bastos, G. Di Natale, M. Flottes, F. Lu, B. Rouzeyre
A New Recovery Scheme against Short-to-Long Duration Transient Faults in Combinational Logic,
Journal of Electronic Testing (JETTA), Springer, DOI: 10.1007/s10836-013-5359-y

[J10] A. Savino, S. Di Carlo, G. Politano, A. Benso, A. Bosio, G. Di Natale
Statistical reliability estimation of microprocessor-based systems,
IEEE Transaction on Computer, Volume PP, Issue 99, October 2011, DOI: 10.1109/TC.2011.188

[J9] G. Di Natale, M. Doulcier, M. L. Flottes, B. Rouzeyre
Self-Test Techniques for Crypto-Devices,
IEEE Transaction on VLSI Systems, pp. 1-5, 2009, DOI: 10.1109/TVLSI.2008.2010045

[J7] A. Benso, A. Bosio, S. Di Carlo, G. Di Natale, P. Prinetto
March Test Generation Revealed,
IEEE Transaction on Computer, Volume 57, Issue 12, Dec. 2008 Page(s):1704 - 1713, DOI: 10.1109/TC.2008.105