Prof. Lilian Bossuet

Citizenship: French
Gender: Male
Marital Status: Martied, Two children (ages 7, 4)
Birth date: October 23, 1975, Angouleme, France

ADRESSES

Laboratoire Hubert Curien
18 rue Benoit Lauras
42000 SAINT ETIENNE – France
Tel : +33 4 77 91 57 92 / +33 6 10 71 20 06
e-mail: lilian.bossuet@univ-st-etienne.fr
www: http://labh-curien.univ-st-etienne.fr/~bossuet/

EDUCATION

H.D.R. (French Accreditation to Supervise Research) in Electrical Engineering University of Bordeaux, France, 06/10
Thesis: Contribution to Reconfigurable Digital System Design – From the Design Space Exploration to the Harware Security
Advisor: Professor Dominique Dallet

Ph.D. in Electrical Engineering
University of South Brittany, Lorient, France, 09/04
Thesis: Design Space Exploration of Reconfigurable Architecture
Advisors: Professor Jean-Luc Philippe and Professor Guy Gogniat

M.Sc in Electrical Engineering
National Institute of Applied Sciences, Rennes, France, 06/01
Top of the class
Thesis : Design Space Exploration of Field Programmable Gate Array
Advisor: Professor Guy Gogniat

National Competitive Examination for Teacher Training in Electrical Engineering (French "*agrégation*")
Ecole Normale Supérieure, Cachan, France, 06/00
Top of the class, top of the competition

PROFESSIONAL EXPERIENCE

09/10 – present **University Jean Monnet Saint-Etienne, France**
Professor (since 09/17) / Associate Professor (10-17) of Electrical and Computer Engineering

Teaching in Telecom Saint-Etienne engineering school. Developed new curricula and course for hardware security.
Researcher in Laboratoire Hubert Curien (CNRS UMR 5516).
Head of the Computer Science Department of the Laboratoire Hubert Curien (since 2016).
Conducted ANR-funded and European-funded research in hardware security, war against illegal IC copy and counterfeiting, IP protection, PUF design and characterization, side channel attacks and countermeasures, TRNG attack, crypto-processor architecture and design, FPGA security.

09/15 – 09/18 **National Center for Scientific Research (CNRS), France**
Part-time (50%) Associate Researcher

09/10 – 09/15 **National Center for Scientific Research (CNRS), France**
Associate Researcher, Chair of Applied Cryptography and Embedded System Security

09/05 – 09/10 **Bordeaux Institute of Technology, France**
Head of the Embedded System Department (2008-2010)
Associate Professor of Electrical and Computer Engineering
Teaching in ENSEIRB-MATLECA engineering school. Developed new curricula for embedded system, digital system design, hardware security.
Researcher in Laboratoire IMS (CNRS UMR 5218)
Conducted research in IP protection, MCryptoPSoC architecture and design, reconfigurable systems architecture and design, ADC design and test.

06/05 – 09/05 **University of Massachusetts, Amherst, USA**
Visiting Researcher on the topic of embedded system security

09/04 – 09/05 **University of South Brittany, Lorient, France**
Assistant Professor in Electrical and Control Engineering
Teaching in in Electrical Engineering Department of Professional Institute of Technology. Developed new courses for FPGA architecture, design and use.
Researcher in Laboratoire Lab-STICC (CNRS UMR 6285). Conducted research in reconfigurable systems architecture and design, FPGA security.

06/05 – 09/05 **University of Massachusetts, Amherst, USA**
Visiting Researcher on the topics of design space exploration of a tile-base reconfigurable architecture and SRAM FPGA security.

09/01 – 09/04 **University of South Brittany, Lorient, France**
Research assistant in Laboratoire Lab-STICC (CNRS UMR 6285). Work involved development of a design space exploration method for designing efficient coarse-grained reconfigurable architecture.

09/01 – 09/04 **University of South Brittany, Lorient, France**
Teaching assistant in Electrical Engineering Department of Professional Institute of Technology.

09/01 – 09/04 **University of Rennes, France**
Teaching assistant in Electrical Engineering Department of University Institute of Technology.

RESEARCH INTERESTS

Primary interest lie in hardware security with a focus on (1) embedded system security, (2) intellectual property protection of fabless designers and IP designers, (3) crypto-processor architecture and design, (4) PUF design and characterization, and (5) security of reconfigurable architecture

HONORS AND AWARDS

2016: **Grand Prix de l'Electronique Général Ferrié**

2015: **IEEE Senior Member Elevation** (only 9% of the IEEE's members hold this grade)

2012: **Outstanding Research Award** – Saint-Etienne Metropolis 2012

2016: **French PEDR Outstanding Research Award** (5-year grant)

2011: **French PES Outstanding Research Award** (5-year grant)

2006: **French PEDR Outstanding Research Award** (5-year grant)

GRADUATE STUDENTS

Current Ph.D Students

1. Fabien Majeric: Hardware attacks on embedded microprocessor (co-advised with E. Bourbao, GEMALTO)
2. Ugo Murredu: A complete framework for the development of physical unclonable functions
3. Mehdi Benhani: TEE security evaluation (co-advised with A. Aubert)
4. Julie Roux: Aerospace system safety evaluation (co-advised with V. Beroulle, INPG)

Ph.D. Graduates

1. Brice Colombier: IP Protection (co-advised with D. Hely, INPG)
2. Cédric Marchand: Design of Salutary Hardware (Salware) to fight against IC counterfeiting and theft (now Associate Professor at Ecole Centrale de Lyon)
3. Pierre Bayon: TRNG Electromagnetic Attacks (now Security Expert at Brightsight)
4. Zouha Cherif: Modelization and Characterisation of PUF (now Engineer at Mentor Graphic)
5. Najeh Kamoun Masmoudi: DPA Countermeasure (now Associate professor at INSA Tunis)
6. Michael Grand: MCryptoPSoC Design for Software Radio (now Security Expert at SERMA Technologies)
7. Nicolas Mechouk: BIST for ADC (now Engineer at THALES Communication and Security)
8. Vincent Fresnaud: No-Linear Error Correction for ADC (now Technical Manager at NXP)
9. Maher Jridi: Mismacht Error correction for Time-Interleaved ADC (now Associate Professor at ISEN Brest)

M.Sc. thesis Graduates

1. Brice Colombier: Remote activation of IP (Pursuiving Ph.D. program with me)
2. Lu Zhao: Electromagnetic Analysis of Ring-Oscillators (Pursuiving Ph.D. program at University of Rouen)
3. Xuan Thuy Ngo (Pursuiving Ph.D. program at Telecom ParisTech)
4. Romain Sacheau: Reconfigurable Architecture for Software Radio

5. Aurélien Ribon: Reconfigurable Routing Node for Ad-hoc Network (Poursuiving Ph.D. program at University of Bordeaux)
6. Hei-Hang Lui: DPA attacks on AES with FLASH-based FPGA implementation
7. Quentin Grison-Boue: Dynamic Partial Reconfiguration of SRAM FPGA
8. Alberto Wiltgen: Hardware Implementation of Public Key Cryptography
9. Houssem Magrhebi: Selft-Adaptive Routing Algorithm for Sensor Network (Poursuiving Ph.D. program at Telecom ParisTech)
10. Zeinab Bouchehiou: Intellectual Property Protection of Software
11. Michael Grand: Hardware Implementation of Key Exchange Cryptographic Protocol (Poursuiving Ph.D. program with me)
12. Fayrouz Haddad: DE2 Board Peripheral Control Unit
13. Brice Heriard-Dubreuilh: Lightweight Hardware Implementation of a FFT
14. Mehres Selmi: DPA Attack on a FPGA implementation of AES
15. Pierre-Marie Robin: Hardware Implementation of AES
16. Ourda Abdaoui: Design Space Exploration with Design Trotter
17. Jérémie Guillot: Bitstream Protection of SRAM FPGA (Poursuiving Ph.D. at University of South Britanny)
18. Samuel Rouxel: Impact of the Routing on FPGA Performances (Poursuiving Ph.D. at University of South Britanny)

Ph.D. Committee Memberships

1. **Comittee President** – Maria Méndez Real, Université Européenne de Bretagne, CS, 2017
2. **Reviewer** – Jérémy Métairie, Université Européenne de Bretagne, CS, 2016
3. **Reviewer** – Xuan Thuy NGO, Telecom Paris Tech, ECE, 2015
4. **Reviewer -** Thomas Peyret, Université Européenne de Bretagne, ECE, 2014
5. **Reviewer -** Karim Abdellatif, Université Pierre et Marie Curie, ECE, 2014
6. **Reviewer -** Stéphanie Kerckhof, Université Catholique de Louvain, Belgique, ECE, 2014
7. **Reviewer -** Thomas Chabrier, Université de Rennes, CS 2013
8. **Reviewer -** Florian Devic, Université de Montpellier, ECE 2012
9. **Reviewer -** Moez Kthiri, Université de Bordeaux, ECE 2012
10. **Reviewer -** Jéremie Crenne, Université Européenne de Bretagne, ECE 2011
11. **Examiner -** Foued Sahraoui, Université de Cergy-Pontoise, ECE 2016
12. **Examiner -** Pramod Udupa, Université de Rennes, ECE 2014
13. **Examiner -** Aurélien Ribon, Université de Bordeaux, ECE 2012
14. **Examiner -** Lubos Gaspar, Université Jean Monnet, Saint-Etienne, ECE 2012

FUNDING

Summary:

I have 5 active grants and contracts, I had 22 past grants and contracts with sources including European Union, OTAN, EIT-ICT, French ANR, French FRAE, DGA, Telecom Institute, Auvergne-Rhône-Alpes Région, Aquitaine Région, ESEO, Pôle AESE, Bordeaux Institute of Technology, and companies such as GEMALTO, Orange Labs, SAFT, NXP, totaling over €3.5 million in funding.

Current:

European Union, H2020 Project HECTOR *Hardware Enable Crypto and Randomness***,** €490,000, 2015-2018

FUI, Project PILAS *Procédé d'injection laser avancés***,** €300,000, 2016-2019

FUI, Project TEEVA *Trusted Execution EVAluation***,** €111,000, 2015-2018

Auvergne-Rhône-Alpes Research Project, VASOC *IoT Security***,** € 66,000, 2017-2021

Auvergne-Rhône-Alpes Research Project, SAFAIR *Aircraft System Safety***,** 2017-2021

Previous:

ANR-FRAE, JCJC Project SALWARE *Salutary Hardware to Fight against IC Counterfeiting and Theft***,** €167,000, 2013-2017

Rhône-Alpes, ARC6 Project *IP Protection***,** €100,000, 2014-2017

ANR, INS Project TSUNAMY *Hardware and Software Management of Data Security in a Manycore Platform***,** €172,000, 2013-2017

GEMALTO, contract *Hardware Attacks on Embedded Processor***,** €25,000, 2014-2017

OTAN, SPS Project SIPQC *Secure Implementation of Post-Quantum Cryptography***,** €190,000, 2013-2016

EIT-ICT, Action line PST *Identidy and Access Management for the Internet of Things***,** €80,200, 2014

ANR, ARPEGE Project EMAISeCi *Electromagnetic Anlysis and Injection of Secure Circuits***,** €160,000, 2010-2014

ANR, ARPEGE Project SecReSoC *Secure Reconfigurable Systems on Chip***,** €130,000, 2009-2013

Telecom Institute, F&R Project SCALA *Random Sources for Cryptography***,** €78,000, 2010-2013

Orange Labs, contract *Random Sources for Cryptography***,** €60,000, 2010-2013

DGA, contract *Research on TRNG***,** €164,000, 2010-2012

DGA, contract *Research on Security for Software Radio***,** €100,000, 2007-2010

ANR, PREDIT Project LIFEMIT *Lithium-Ion Battery for Military Transportation Applications***,** €103,000, 2008-2011

Aquitaine, pôle AESE Project PLUS *Unisource Localisation***,** €538,000, 2008-2010

ESEO-Aquitaine, **pôle AESE Project SYMM** *Micro-UAV design*, €100,000, 2009-2010

Bordeaux Institute of Technology, *Reconfigurable Gateway for Sensor Network*, €16,000, 2008-2010

Bordeaux Institute of Technology, *Self Management of Ad-hoc Sensor Network*, €27,000, 2007-2010

NXP, contract *ADC Folding Interpolating***,** €115,000, 2005-2008

DGA, REI *Time-Interleaved ADC***,** €128,000, 2007-2008

SAFT, contract *Mathodology of Intellectual Property Protection***,** €10,000, 2007-2008

TEACHING

Summary:
I teach since 18 years mainly at post-graduate level in several institutions including Telecom Saint-Etienne, Bordeaux Institute of Technology, University of South Britanny, University of Bordeaux, University of Rennes, Ecole Centrale de Lyon, Ecole Normale Supérieure de Cachan, SupCom Tunis, totaling over 2,836 hours in teaching.

Courses taught at Telecom Saint-Etienne, Post-Graduate Level (Fall 2010 – Present)

- ABCD Analog Electronic
- ELEC2 Digital system design
- ELEC5 Hardware security
- ELEC5 Reconfigurable Architecture

Courses taught at Bordeaux Institute of Technology, Post-Graduate Level (Fall 2005 – 2010)

- EN 102 Boolean logic
- EN 103 Digital system design
- EN 104 Micro-processor I
- EN 105 Micro-processor II
- EN 112 Digital system design
- MI 100 Processor architecture
- EN 201 Logic synthesis
- EN 202 VHDL project
- EN 202 Micro-processor III
- EN 204 Micro-processor IV
- EN 208 VLSI design
- EN 211 M2M communications
- MI 200 FPGA
- EN 107 FPGA-VHDL
- EN 108 Digital system design
- EN 309 Digital signal processing
- EN 312 Digital communications
- EN 310 Advanced digital communications
- ME 333 VLSI design
- ME 333 Low power design
- EN 314 Hardware security

- ME 330 Embedded system security
- PR 205 Telecommunication
- PR 309 Network
- PR 309 Digital signal processing

Courses taught at others institutions, Post-Graduate Level

- Hardware security – Ecole Centrale de Lyon
- Embedded system security – SupCom Tunis, Tunisie
- Applied Cryptography – University of Bordeaux
- FPGA Design – Ecole Normale Supérieure de Cachan
- Digital system design – University of South Britanny
- Control Engineering – University of South Britanny

Courses taught at others institutions, Undergraduate Level

- Electronic – University of Rennes
- Digital System Design – University of Rennes

SERVICE TO DEPARTEMENT AND THE UNIVERSITY

Elected member of the board of directors of the Univ. Jean Monnet (20 000 students, five faculties, four institutes) 2015-2017.

Invited member of the board of directors of ENSEIRB-MATMECA (1 000 students, six departments) since 2008-2010.

Head of the Embedded System Department of Bordeaux Institute of Technology, 2008-2010. I headed a team of teaching staff composed by four permanent teachers and two assistants responsible for around 75 students.

Scientific Committees: ENSEIRB-MATMECA (2009-2010), Univ. of South Britany (2001-2003).

EE Graduate Curriculum Committee: Telecom Saint-Etienne (head, 2010-present), MASTER EEAP INSA Lyon (2010-present), ENSEIRB-MATMECA (2005-2010)

Recruitment Committee of Associated Professor (Evaluator): Univ. of South Britany (2014, 2011 and 2010), Grenoble Inst. of Tech. (2014), Bordeaux Inst. of Tech. (2012 and 2011), Univ. of Montpellier (2012), Univ. of Saint-Etienne (2016, 2011), Univ. of Bordeaux (2010, 2009, 2008 and 2007).

PROFESSIONAL ACTIVITIES

I'm particularly involved in the French CNRS scientific network on System-On-Chip, Embedded Systems and Connected Things (GDR SoC²): Board of Directors (2014-present), Strategy Committee (2014-present), Leader of the Security and Safety of System (2014-present), Leader of the Hardware Security Working Group (2013-present).

I'm particularly involved in the French CNRS scientific network on Computing Security (GDR Sécurité Informatique): Board of Directors (2017-present), Leader of the Hardware Security Working Group (2017-present).

I was involved in the European scientific network of excellence on Trustworthy Manufacturing of Secure Devices COST-ACTION TRUDEVICE: Leader of the Working Group Trustworthy Manufacturing of Secure Devices (2013-2017).

I was involved in IDEFI CNFM FINMINA Strategy Committee (2014-2017)

I'm or I was involved in many conferences/journals committee:

Program Chair Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (DATE Workshop) 2015

Security Track Chair of IFIP/IEEE International Conference on Very Large Scale Integration, VLSI-SoC (2016-present)

Guest Editor Special Issue on Trustworthy Manufacturing and Utilization of Secure Devices, ELSEVIER Microprocessors end Microsystems, 2015

Program Committee of SEmba day of Rhône-Alpes

Program Committee of Workshop on Reconfigurable Communication Centric Systems-on-Chip (ReCoSoC)

Program Committee of International Workshop on cryptographic Architectures Embedded in Reconfigurable Devices (CryptArchi)

Program Committee of Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)

Program Committee of Training School on TRUDEVICE.

Program Chair of the Special Session on Hardware-based Security, IEEE International NEWCAS Conference 2011

Program Chair of the Special Session on Reconfigurable Computing in Education, International Workshop on Reconfigurable Communication Centric System-on-Chip, ReCoSoC 2011

Program Chair of the Special Session on Security Evaluation and Protection of Cryptographic Devices, IEEE International Signals, Circuits and Systems Conference, SCS 2009

Program Chair of the Special Session on Digital System, IEEE International Conference on Electronics, Circuits and Systems Conference, ICECS 2006

REFEREE/REVIEWER FOR

Natural Sciences and Engineering Research Council of Canada (NSERC),

French National Scientific Agency (ANR),

Région Auvergne Rhône-Alpes

REVIEWER FOR

IEEE Transactions on Computers

IEEE Transactions on Information Theory

IEEE Transactions on Circuits and Systems
ACM Transactions on Reconfigurable Technology and Systems
ACM Transactions on Embedded Computing Systems
EIT Computers & Digital Techniques
SPRINGER Journal of Cryptographic Engineering
ELSEVIER Microprocessors and Microsystems
EURASIP Journal of Embedded System

IEEE International Symposium on Circuits and Systems
IEEE Computer Society Annual Symposium on VLSI
IEEE VLSI Test Symposium
IEEE International NEWCAS Conference
Design Automation, & Test in Europe
IEEE Conference on Design of Circuits and Integrated Systems
IEEE International Conference on Electronics, Circuits and Systems Conference
IEEE International Signals, Circuits and Systems Conference

International Symposium on Applied Reconfigurable Computing
International Workshop on constructive Side-Channel Analysis and Secure Design
Workshop on Cryptographic Hardware and Embedded Systems
Workshop on cryptographic Architectures Embedded in Reconfigurable Devices
International Conference on Field Programmable Logic and Applications
International Conference on Engineering of Reconfigurable Systems and Algorithms
International Conference on Computer and Communication Technology
Reconfigurable Architecture Workshop
International Conference on ReConFigurable Computing and FPGAs
International Workshop on Reconfigurable Communication Centric System-on-Chip
Conference on Design and Architecture for Signal and Image Processing

INVITED TALKS

[20] L. Bossuet. Evaluation de la sécurité de la technologie ARM TrustZone. Ecole d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes, FETCH 2018, Saint-Malo, France, Janvier 2018.

[19] L. Bossuet. Confiance numérique. Séminaire "Risques, société et sécurité", Université de Cergy-Pontoise, France, Mars 2017.

[18] L. Bossuet. La sécurité des systèmes embarqués. Ecole technologique du réseau des électroniciens du CNRS, Bordeaux, France, Octobre 2016.

[17] L. Bossuet. *La lutte contre le vol, la copie et la contrefaçon de circuits intégrés*. Séminaire "Confiance Numérique", Université de Clermont Ferrand, France, Mars 2016.

[16] L. Bossuet. *La sécurité des objets connectés : les défis matériels*. Colloque Objets Connectés, dans le cadre des Entretiens Jacques Cartier 2015, Lyon, France, Décembre 2015.

[15] **Tutorial** V. Fischer, L. Bossuet, J.L. Danger. *Underneath the FPGA Clothes: Enhancing Security*. Tutorial of the 25th International Conference Field Programmable Logic and Applications, FPL'03, Imperial College, London, United Kindom, September 1st, 2015.

[14] **Keynote** L. Bossuet. *Salutary Hardware – a state of the art*. Ecole d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes, FETCH 2015, Louvain-la-Neuve, Belgique, Janvier 2015.

[13] L. Bossuet. *Fighting against Theft, Cloning and Counterfeiting of Integrated Circuits*. Séminaire "Sécurité des Systèmes Electroniques Embarqués", DGA-MI, IRISA, Rennes, France, Mai 2015.

[12] C. Marchand, L. Bossuet. *Analyse de la consommation de puissance appliquée à la vérification du marquage d'IP*. Journée sécurité numérique du GDR SoC-SiP, Paris, France, Décembre 2014.

[11] L. Bossuet. *Hardware Access Control in Constrained Environments*. Conference on sensors energy harvesting wireless network and smart object (SENSO), Gardanne, France, Octobre 2014.

[10] L. Bossuet. *Sustainable Electronics: on the Trail of Reconfigurable Computing*. Workshop on computing and the environment, Banyuls-sur-Mer, France, Octobre 2014.

[9] L. Bossuet. *The Fight against Theft, Cloning and Counterfeiting of Integrated Circuits*. TRUDEVICE Summer and Training School, Lisbonne, Portugal, Juillet 2014.

[8] L. Bossuet. *Fighting against Theft, Cloning and Counterfeiting of Integrated Circuits*. Séminaire de l'Université Catholique de Louvain-la-Neuve, Belgique, Mai 2014.

[7] L. Bossuet. *SALWARE: Salutary Hardware to Design Trusted IC*. Ecole d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes, FETCH 2014, Ottawa, Canada, Janvier 2014.

[6] L. Bossuet. *Hardware Security Design – From Secure Architecture to Secure Logic*. XXVII Conference on Design of Circuits and Integrated Systems, DCIS 2012, Avignon, France, November 2012.

[5] L. Bossuet. *Lutte contre le vol, la copie illégale, le reverse-engineering et la contrefaçon de circuits intégrés*. Journée sécurité numérique du GDR SoC-SiP, Paris, France, Novembre 2012.

[4] L. Bossuet. *Engins matériels cryptographiques flexibles et embarqués : vers les MCryptoPSoC sécurisés*. Ecole d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes, FETCH 2012, Alpe d'Huez, France, Janvier 2012.

[3] P. Bayon, L. Bossuet. *La generation d'aléa : une cible potentielle des attaques par analyse du rayonnement électromagnétique*, Journée Sécurité du GDR SoC-SiP, Paris, France, 18 mai 2011.

[2] L. Bossuet. *Architectures et tendances des FPGA*. Ecole thématique, architectures des systèmes matériels enfouis et méthodes de conception associées, ARCHI 2009, Pleumeur-Bodou, France, April 2009.

[1] L. Bossuet, N. Kamound, A. Gazel. *A Very Low Cost DPA Countermeasures to Secure Hardware AES Cipher*. Selected Long Talk of the International CryptArchi Workshop 2009, pp. 72-77, Prague, Czech Republic, 24-27 June 2009.

BOOK:

[1] L. Bossuet, L. Torres (Eds). Foundations of Hardware IP Protection. Springer, 2017 (10 Chapters, 240 pages). ISBN : 978-3-319-50378-3

BOOK CHAPTERS:

[14] L.Torres, P. Benoit, J. Rampon, R. Perillat, D. Spring, G. Paul, S. Bonniol L. Bossuet. Digital Right Management for IP Protection. Foundations of Hardware IP Protection, L. Bossuet, L. Torres, Springer, 2017 (Chapter 1: 14 pages). ISBN : 978-3-319-50378-3

[13] B. Colombier, L. Bossuet. Turning Electronic Circuits Features into On-Chip Locks. Foundations of Hardware IP Protection, L. Bossuet, L. Torres, Springer, 2017 (Chapter 2: 22 pages). ISBN : 978-3-319-50378-3

[12] B. Colombier, L. Bossuet. Logic Modification-Based IP Protection Methods: an Overview and a Proposal . Foundations of Hardware IP Protection, L. Bossuet, L. Torres, Springer, 2017 (Chapter 3: 27 pages). ISBN : 978-3-319-50378-3

[10] E. Jung, L. Bossuet. IP FSM Watermarking. Foundations of Hardware IP Protection, L. Bossuet, L. Torres, Springer, 2017 (Chapter 4: 21 pages). ISBN : 978-3-319-50378-3

[9] L. Bossuet, C. Marchand. Side Channel Analysis, an Efficient Ally for IP Protection. Foundations of Hardware IP Protection, L. Bossuet, L. Torres, Springer, 2017 (Chapter 5: 21 pages). ISBN : 978-3-319-50378-3

[8] C. Marchand, L. Bossuet; K. Gaj. Ultra-Lightweight Implementation in Area of Block Ciphers. Foundations of Hardware IP Protection, L. Bossuet, L. Torres, Springer, 2017 (Chapter 9: 27 pages). ISBN : 978-3-319-50378-3

[7] L. Bossuet, P. Bayon, V. Fischer. Contacless Transmission of Intellectual Property Data to Protect FPGA Designs. VLSI-SoC: Design for Reliability, Security and Low Power, Y. Shin, C. Y. Tsui, J.J. Kim Kiyoung Choi, and R. Reis, Springer, 2016 (Chapter 8: 21 pages).

ISBN 978-3-319-46096-3

[6] L. Bossuet, P. Bayon, V. Fischer. Attacking on-chip oscillators in cryptographic applications. Oscillator Circuits: Frontiers in Design, Analysis and Applications, Y. Nishio, IET Book, December 2016 (Chapter 14: 22 pages).

ISBN: 978-1-78561-057-8

[5] L. Bossuet. *Reconfigurable Green Terminals: a Step Towards Sustainable Electronics*. Green Networking, F. Krief, Wiley-ISTE, Aout 2012 (Chapter 7: 38 pages).
ISBN : 978-1-84821-378-4

[4] L. Bossuet. *Chapitre 7 : Des terminaux green reconfigurables – vers une électronique durable*. Traité IC2, série réseaux et télécoms. Le Green Networking vers des réseaux efficaces en consommation énergétique, sous la direction de Francine Krief, aux éditions Hermes Science, septembre 2012, (Chapitre 7 : 29 pages).

ISBN: 978-2746232754

[3] L. Bossuet, G. Gogniat. *Hardware Security in Embedded Systems*. Communicating Embedded Systems for Networks, F. Krief, Wiley-ISTE, April 2010 (Chapter 5: 36 pages).
ISBN: 978-1-84821-144-5

[2] L. Bossuet, G. Gogniat. *Chapitre 5 : La sécurité matérielle des systèmes embarqués*. Traité IC2, série réseaux et télécoms. Les systèmes embarqués communicants : mobilité, sécurité, autonomie, sous la direction de Francine Krief, aux éditions Hermes Science, septembre 2008, 306 pages (Chapitre 5 : 31 pages).
ISBN: 978-2746218734

[1] L. Bossuet, G. Gogniat, J.L. Philippe. *System-onChip for Real Time Applications (chapter 4 : modeling)*. The Kluwer International Series in Engineering and Computer Science, Vol. 711. Wael Badawy, Graham A. Julien (Eds). 480p, 2003.
ISBN 1-4020-7254-6

JOURNALS:

[32] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, V. Fischer. Implementation and characterization of a physical unclonable function for IoT: a case study with the TERO-PUF, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE Council on Electronic Design Automation (CEDA), Vol. 37, No. 1, pp. 97-109, January 2018.

[31] F. Majeric, B. Gonzalvo, L. Bossuet. JTAG Fault Injection Attack, IEEE Embedded Systems Letters, available online November 2017.

[30] B. Colombier, L. Bossuet, V. Fischer, D. Hely. Key Reconciliation Protocols for Error Correction of Silicon PUF Responses, IEEE Transactions on Information Forensics and Security, IEEE Signal Processing Society, Vol. 12, No. 8, pp. 1988-2002, August 2017.

[29] C. Reinbrecht, A. Susin, L. Bossuet, G. Sigl, J. Sepulveda. Timming Attack on NoC-based Systems: Prime+Probe Attack and NoC-based Protection, Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, Vol. 52, pp. 556-565, July 2017.

[28] C. Marchand, L. Bossuet, K. Gaj. Area-oriented Comparison of Lightweight Block Ciphers Implemented in Hardware for the Activation Mechanism in the Anti-counterfeiting Schemes, International Journal of Circuit Theory and Applications, Wiley, Vol. 45, No. 2, pp. 274-291, February 2017.

[27] L. Bossuet. La lutte contre le col, la copie et la contrefaçon de circuits intégrés. Revue de l'Electricité et de l'Electronique, SEE, vol. 2017-1, pages 5-10, février 2017.

[26] E. Jung, L. Bossuet, S. Choi, C. Marchand. Identification of IP Control Units by State Encoding and Side Channel Verification, Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, Vol. 47, Part A, pp. 11-22, November 2016

[25] L. Bossuet, N. Datta, C. Mancillas Lopez, M. Nandi, ELmD: A Pipelineable Authenticated Encryption and Its Hardware Implementation. IEEE Transactions on Computer, IEEE Computer Society, Vol. 65, No. 11, pp. 3318-3331, November 2016

[24] B. Colombier, L. Bossuet, D. Hely. From Secured Logic to IP Protection. Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, Vol. 47, Part A, pp. 44-54, November 2016.

[23] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. *Fault model of electromagnetic attacks targeting ring oscillator-based true random number generators.* Journal of Cryptographic Engineering, Springer, Vol. 6, No. 1, pp. 61-74, April 2016.

[22] A. Cherkaoui, L. Bossuet, C. Marchand, *Design, Evaluation and Optimization of Physical Unclonable Functions based on Transient Effect Ring Oscillators,* IEEE Transactions on Information Forensics and Security, IEEE Signal Processing Society, Vol. 11, No. 6, pp. 1291-1305, June 2016.

[21] L. Bossuet, B. Colombier, *A Comment on "PUF-FSM Binding Scheme for FPGA IP Protection and Pay-per-Device Licensing"* IEEE Transactions on Information Forensics and Security, IEEE Signal Processing Society, *accepted in October 2015, to be published soon.*

[20] L. Bossuet, P. Bayon, V. Fischer. *An ultra-lightweight BFSK transmitter using an electromagnetic channel for salware or malware.* IEEE Embedded Systems Letters, accepted in July 2015 (available online). Doi: 10.1109/LES.2015.2454236.

[19] L. Bossuet, V. Fischer, L. Gaspar, L. Torres, G. Gogniat. *Disposable Configuration of Remotely Reconfigurable Systems.* Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, Vol. 39, No. 6, pp. 382-392, August 2015. Doi: 10.1016/j.micpro.2015.05.007.

[18] L. Bossuet, V. Fischer, L. Gaspard, G. Gogniat, L. Torres. *Disposable Configurable of remotely Reconfigurable Systems.* Elsevier Microprocessors and Microsystems, *to be published in 2015*

[17] B. Colombier, L. Bossuet. *A survey of hardware protection of design data for integrated circuits and intellectual properties.* IET Computers & Digital Techniques, Vol. 8, No. 6, pp. 274-287, Novembre 2014. Doi: 10.1049/iet-cdt.2014.0028

[16] L. Bossuet. *Sustainable electronics: on the trail of reconfigurable computing.* Elsevier Sustainable Computing: Informatics and Systems, Vol. 4, No. 3, pp. 196-202, September 2014.

[15] L. Bossuet, X. T. Ngo, Z. Cherif, V. Fischer. *A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon.* IEEE Transactions on Emerging Topics in Computing, Vol. 2, Issue 1, pp. 30-36, *2014.*

[14] L. Bossuet, M. Grand, L. Gaspar, V. Fischer, G. Gogniat. *Architectures of flexible symmetric key crypto engines – a survey : from hardware coprocessor to multi-crypto-processor system on chip.* ACM Computing Surveys, Vol. 45, No. 4, Article 41, 32 pages, Aout 2013.

[13] L. Gaspar, V. Fischer, L. Bossuet, R. Fouquet. *Secure extensions of FPGA general-purpose processors for symmetric key cryptography with partial reconfiguration.* ACM Transactions on Reconfigurable Technology and Systems, Vol. 5, No 3, Article 16, 13 pages, October 2012.

[12] B. Le Gal, L. Bossuet. *Automatic low-cost IP watermarking technique based on output mark insertion.* Design Automation for Embedded System, Springer, Vol. 16, No. 2, pp. 71-92, June 2012.

[11] L. Bossuet. *Approche didactique pour l'enseignement de l'attaque DPA ciblant l'algorithme de chiffrement AES.* Journal sur l'enseignement des sciences et technologies de l'information et des systèmes (j3ea), EDP Sciences, vol. 11, octobre 2012.

[10] N. Kamoun, L. Bossuet, A. Gazel. *Implementation of DPA Attacks on Flash-Based FPGA Hardware AES Cipher and Proposal of a Novel Correlated Power Noise Generator Countermeasures*. Shaker-Verlag Transactions on Systems, Signals and Devices, Issues on "Sensors, Circuits and Instrumentations Systems", Vol. 5, No. 4, pp. 359-380, December 2011.

[9] V. Kerzérho, V. Fresnaud, D. Dallet, S. Bernard, L. Bossuet. *Fast Digital Post-processing Technique for INL Correction of ADC : Validation on a 12 bit F&I ADC*. IEEE Transactions on Instrumentation and Measurement, Vol. 60, Issue 3, pp. 768-775, 2011. doi: 10.1109/TIM.2010.2060222.

[8] B. Le Gal, L. Bossuet, M. Grand. *Enseignement ludique de la programmation objets à l'aide des applications de traitement d'image*. Journal sur l'enseignement des sciences et technologies de l'information et des systèmes (j3ea), EDP Sciences, vol.10, juin 2011.

[7] L. Bossuet. *Sécurité de la configuration des FPGA (SRAM et FLASH).* Multi-System & Internet Security Cookbook*,* Ed. Diamond, Numéro 46, pages 18-22, novembre-décembre 2009.

[6] G. Gogniat, T. Wolf, W. Burleson, J.P. Diguet, L. Bossuet, R. Vaslin. *Reconfigurable hardware for high-security/high-performance embedded systems: The SAFES perspective*. In IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume 16, Issue 2, pp. 144-155, Februrary 2008. Doi: 10.1109/TVLSI.2007.912030.

[5] L. Bossuet, G. Ferre. *Etude et modélisation sous Simulink d'une chaine de transmission DVB-S*. Journal sur l'enseignement des sciences et technologies de l'information et des systèmes (j3ea), EDP Sciences, vol.7, septembre 2008.

[4] L. Bossuet, G. Gogniat, J.L. Philippe. *Communication-Oriented Design Space Exploration for Reconfiguration Architecture*. In Eurasip Journal of Embedded System, from Hindawi Publishing Corporation, vol. 2007, Article ID 23496, 20 pages, 2007. doi:10.1155/2007/23496.

[3] L. Bossuet, G. Gogniat, W. Burleson. *Dynamically Configurable Security for SRAM FPGA Bitstreams*. In International Journal of Embedded Systems, IJES, from Inderscience Publishers, Vol. 2, Nos. 1/2, pp 73-85, 2006.

[2] S. Bilavarn, G. Gogniat, J.L. Philippe, L. Bossuet. *Design Space Pruning Through Early Estimations of Aera/Delay Tradeoffs for FPGA Implementations*. In IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, ITCAD, Vol. 25, No 10, pp 1950-1968, October 2006. Doi: 10.1109/TCAD.2005.862742.

[1] L. Bossuet, G. Gogniat, J.L. Philippe. *Exploration de l'espace de conception des architectures reconfigurables*. Revue des Technique et Science Informatiques, série TSI, Architecture des ordinateurs, Hermes Lavoisier, Volume 25 – n°7/2006, pp 921-946, Octobre 2006.
ISBN : 2-7462-1627-2

REFEREED CONFERENCES

[65] B. Colombier, L. Bossuet, D. Hely. A comprehensive hardware/software infrastructure for IP cores design protection. In Proceedings of the IEEE International Conference on Field-Programmable Technology, ICFPT 2017, Melbourne, Australia, December 2017.

[64] E.M. Benhani, C. Marchand, L. Bossuet, A. Aubert. On the Security Evaluation of the ARM TrustZone Extension in a Heterogeneous SoC. 30th IEEE International System-on-Chip Conference, SOCC 2017, Munich, Germany, September, 2017.

[63] B. Ovilla-Martinez, L. Bossuet. Restoration protocol: Lightweight and secure devices authentication based on PUF. IFIP/IEEE International Conference on Very Large Scale Integration, VLSI-SoC 2017, UAE, October, 2017.

[62] U. Mureddu, O. Petura, N. Bochard, L. Bossuet, V. Fischer. Efficient design of Oscillator based Physical Unclonable Functions on Flash FPGAs. 2nd International Verification and Security Workshop, IVSW'17, Thessaloniki, Greece, July 3-5 2017.

[61] B. Colombier, L. Bossuet, D. Hely. Centrality Indicators for Efficient And Scalable Logic Masking. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2017, Bochum, Germany, July 2017.

[60] F. Majéric, E. Bourbabo, L. Bossuet. Electromagnetic security for SoC. In Proceedings of the 23rd IEEE International Conference on Electronics Circuits and Systems, ICECS 2016, Monte Carlo, Monaco, December 2016.

[59] F. Majéric, B. Gonzalvo, L. Bossuet. JTAG Combined Attack. In Proceedings of the 8th IFIP International Conference on New technologies, Mobility & Security, NTMS 2016, Larnaca, Cyprus, November 2016.

[58] O. Petura, U. Mureddu, N. Bochard, V. Fischer, L. Bossuet. A Survey of AIS-20/31 compliant TRNG Cores Suitable for FPGA Devices. In Proceedings of the 26th International conference on Field-Programmable Logic and Applications, FPL 2016, Lausanne, Switzerland, August 2016.

[57] C. Marchand, L. Bossuet. *Design and characterization of the TERO-PUF on SRAM FPGAs.* In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2016, Pittsburgh, Pennsylvania, USA, July 2016.

[56] C. R. Wedig Reinbrecht, A. Susin, L. Bossuet and M. J. Sepulveda. *Gossip NoC - Avoiding Timing Side-Channel Attacks through Traffic Management.* In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2016, Pittsburgh, Pennsylvania, USA, July 2016.

[55] F. Bruguier, P. Benoit, L. Torres, L. Bossuet. *Hardware Security: from Concept to Application.* In Proceedings of the 11th European Workshop on Microelectronics Education, Southampton, U.K., May 2016.

[54] C. Marchand, L. Bossuet, A. Cherkaoui. *Enhanced TERO-PUF Implementations and Charaterization on FPGAs.* In Proceedings (poster) of the 24th ACM/SIGDA International Symposium on field-Programmable gate Arrays, FPGA 2016, Monterey, USA, Februray 21-23, 2016.

[53] L. Bossuet, V. Fischer, P. Bayon. *Contactless Transmission of Intellectual Property Data to Protect FPGA Designs.* In Proceedings of the 23nd IFIP/IEEE International Conference on Very Large Scale Integration, VLSI-SoC 2015, Korea, November, 2015.

[52] L. Bossuet, N. Datta, C. Mancillas-Lopéz, M. Nandi. *Hardware Performance of ELmD and ELmD(6,6).* In Proceedings of Direction in Authenticated Ciphers, DIAC 2015, Singapore, September 2015.

[51] B. Colombier, L. Bossuet, D. Hely. *Reversible Denial-of-Service by Locking Gates Insertion for IP Cores Design Protection.* In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2015, Montpellier, France, July 2015.

[50] B. Colombier, L. Bossuet. *Functional Locking Schemes for Design Protection of Intellectual Property Cores Embedded in FPGAs.* In Proceedings of the 23rd IEEE International Symposium

on Field-Programmable Custom Computing Machines, FCCM 2015, Vancouver, British Columbia, Canada, May 2015.

[49] E. Jung, C. Marchand, L. Bossuet. *Identification of Embedded Control Units by State Encoding and Power Consumption Analysis*. In Proceedings of the 30th ACM/SIGAPP Symposium on Applied Computing, Salamanca, Spain, April 2015.

[48] C. Mancilla Lopez, M. Mendez Real, L. Bossuet, G. Gogniat, V. Fischer, A. Baganne,. *Trusted Computing using Enhanced Manycore Architectures with Cryptoprocessors* In Proceedings of the 22nd IFIP/IEEE International Conference on Very Large Scale Integration, VLSI-SoC 2014, Mexico, October, 2014.

[47] P. Maistri, R. Leveugle, L. Bossuet, A. Aubert, V. Fischer, B. Robisson, N. Moro, P. Maurine, J-M. Dutertre and M. Lisart. *ElectroMagnetic Analysis and Fault Injection onto Secure Circuits*. In Proceedings of the 22nd IFIP/IEEE International Conference on Very Large Scale Integration, VLSI-SoC 2014, Mexico, October, 2014.

[46] C. Marchand, L. Bossuet, E. Jung. *IP Watermark Verification Based on Power Consumption Analysis*. In Proceedings of the 27th IEEE International Systems-on-Chip Conference, SOCC 2014, Las-Vegas, USA, Septembre 2014.

[45] A. Cherkaoui, L. Bossuet, L Seitz, G. Selander and R. Borgaonkar. *New Paradigms for Access Control in Constrained Environments*. In Proceedings of the IEEE International Symposium on Reconfigurable Communication-centric Systems-on-Chip, ReCoSoC 2014, Montpellier, France, Mai 2014.

[44] L. Bossuet. *Teaching FPGA Security*. In Proceedings of the IEEE International Conference on Field-Programmable Technology, ICFPT 2013, Kyoto, Japan, December 2013.

[43] Z. Cherif, J.L. Danger, F. Lozac'H, Y. Mathieu, L. Bossuet. *Evaluation of delay PUFs on CMOS 65nm technology: ASIC vs FPGA*. International Workshop on Hardware and Architectural Support for Security and Privacy, HASP 2013, Tel-Aviv, Israel, June 2013.

[42] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. *EM radiation analysis on true random number generators: Frequency and localization retrieval method*. In Proceedings of the IEEE Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility, APEMC 2013, Melbourne, Australia, May 2013.

[41] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. *Electromagnetic Analysis on Ring Oscillator-Based True Random Number Generators*. In Proceedings of the IEEE International Symposium on Circuits and Systems, ISCAS 2013, Beijing, China, May 2013.

[40] P. Bayon, F. Poucheret, L. Bossuet, B. Robisson, A. Aubert, P. Maurine, V. Fischer. *Contactless Electromagnetic Active Attack on Ring Oscillator Based true Random Number Generator*. Third International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012, Lecture Notes in Computer Science, Springer, LNCS 7275, pp. 151-166, Darmstadt, Germany, May 2012.

[39] Z. Cherif, J.L. Danger, S. Guilley, L. Bossuet. *A easy-to-design PUF based on a single oscillator: the loop PUF*. 15th Euromicro Conference on Digital System Design, DSD 2012, Cesme, Izmir, Turkey, September 2012.

[38] N. Kamoun, L. Bossuet, A. Gazel. *A Masked Correlated Power Noise Generator as a Second Order DPA Countermeasure to Secure Hardware AES Cipher"*. In the 23rd IEEE International Conference on Microelectronics, ICM 2011, Hammamet, Tunisia, December 2011.

[37] L. Gaspar, V.Fischer, L. Bossuet, M. Drutarovsky. *Cryptographic extension for soft general-purpose processors with secure key management*, In 21st International Conference on Filed Programmable Logic and Applications, FPL 2011, Chania, Crete, Greece, September 5-7 2011.

[36] L. Gaspar, V.Fischer, L. Bossuet, R. Fouquet. *Secure extensions of soft core general-purpose processors for symmetric key cryptography*, In 6th IEEE International Workshop on Reconfigurable Communication-centirc System-on-Chip, ReCoSoC 2011, Montpellier, France, June2011.

[35] B. Le Gal, L. Bossuet. *Low-Cost IP Watermarking Techique Based on I/O Mark Insertions*. In 9th IEEE International NEWCAS conference 2011, pp. 490-493, Bordeaux, France, June 26-29, 2011.

[34] Z. Cherif Jouini, L. Bossuet, J.L. Danger. *Performance Evaluation of Silicon Physically Unclonable Function by Studing Physicals Values*. In 9th IEEE International NEWCAS conference 2011, pp. 482-485, Bordeaux, France, June 26-29, 2011.

[33] M. Grand, L. Bossuet, G. Gogniat, B. Legal, J-P. Delahaye, D. Dallet. *A Reconfigurable Multi-core cryptoprocessor for Multi-channel Communication Systems*. In 18th IEEE Reconfigurable Architectures Workshop, RAW 2011, Workshop of IEEE IPDPS 11, pp. 199-206, Anchorage, Alaska, USA, 16-17 may 2011.

[32] M. Grand, L. Bossuet, B. Le Gal, G. Gogniat, D. Dallet. *Design and Implementation of a Multi-Core crypto-Processor for Software Defined Radios*. In the 7th International Symposium on Applied reconfigurable Computing, ARC 2011, pp. 29-40, Belfast, United Kingdom, March 2011.

[31] L. Gaspar, V.Fischer, F. Bernard, L. Bossuet, P. Cotret. *HCrypt: A Novel Reconfigurable Crypto-processor with Secured Key Management*. In International Conference on ReConFigurable Computing and FPGAs, pp. 280-285, Cancun, Mexico, December 13-15 2010.

[30] N. Mechouck, D. Dallet, L. Bossuet, B. Le Gal. *A Low-Area Filter Bank Design Methodology for On-Chip ADC Testing*. In IEEE International Conference on Electronics, Circuits and Systems, ICECS 2010, pp. 724-727, Athens, Grece, December 12-15 2010.

[29] N. Kamoun, L. Bossuet, A. Gazel. *Experimental Implementation of 2ODPA attacks on AES design with flash-based FPGA Technology*. In the 22nd IEEE International Conference on Microelectronics, IMC 2010, pp. 407-410, Cairo, Egypt, December 2010.

[28] M. Grand, L. Bossuet, B. Le Gal, D. Dallet, G. Gogniat. *A Multi-Core AES Cryptoprocessor for Multi-Channel SDR*. In the Military Communication and Information Systems Conference, MCC 2010, pp. 1-7, Wroclaw, Poland, September 2010.

[27] A. Ribon, B. Le Gal, L. Bossuet, D. Dallet. *Behavioral Assertion Support in HLS Design Flow*. In System, Software, SoC and Silicon Debug Conference, SD4 2010, Southampton, UK. September 2010.

[26] B. Le Gal, A. Ribon, L. Bossuet, D. Dallet. *Reducing and Smoothing Power consumption of ROM-based Controller Implementations*. In 23rd Symposium on Integrated Circuits and Sytems Design, SBCCI 2010, pp. 8-13, Sao Paulo, Brazil, September 2010.

[25] B. Le Gal, L. Bossuet, D. Dallet. *Area Optimization Of ROM-Based Controllers Dedicated To Digital Signal Processing Applications*. In In 18th EURASIP European Conference on Signal Processing 2010, EUSIPCO 2010, Aalborg, Danemark, August 23-27, 2010.

[24] B. Le Gal, L. Bossuet, D. Dallet. *Using Digital Signal Processor Singularities to Minimize ROM Based Controller Area*. In the 8th IEEE International NEWCAS Conference, pp. 29-32, Montreal, Canada, June 2010.

[23] N. Kamoun, L. Bossuet, A. Gazel. *Correlated Power Noise Generator as a Low Costs DPA Countermeasures to Secure Hardware AES Cipher*. In the 3rd IEEE International Conference on Signals, Circuits and Systems, SCS 2009, pp. 1-6, Djerba, Tunisa, November 2009.

[22] M. Grand, L. Bossuet, B. Le Gal, D. Dallet, G. Gogniat. *A Reconfigurable Crypto Sub System for the Software Communication Architecture.* In the IEEE Military Communication Conference, MILCOM 2009, pages 1-7, Boston, Massachusetts, USA, October 2009.

[21] N. Kamoun, L. Bossuet, A. Gazel. *Experimental Implementation of DPA Attacks on AES Design with Flash-based FPGA Technology*. In the Sixth IEEE International Multi-Conference on Systems Signals and Devices, SSD 2009, pp. 1-4, Djerba, Tunisa, March 2009.

[20] N. Kamoun, L. Bossuet, A. Gazel. *SRAM-FPGA Implementation of Masked S-Box Based DPA countermeasure for AES*. In IEEE International Design and Test Workshop, IDT 2008, pp. 74-77, Monastir, Tunisa, December 2008.

[19] G. Ferré, B. Le Gal, L. Bossuet, M. Jridi, D. Dallet and P. Collucci. *Orthogonal correction implementation for time interleaved analog-to-digital converters: realtime application.* In 16th EURASIP European Conference on Signal Processing 2008, EUSIPCO 2008, Lausanne, Switzerland, August 25-29, 2008.

[18] G. Ferre, M. Jridi, L. Bossuet, B. Le Gal and D. Dallet. *A New Orthogonal Online Digital Calibration for Time-Interleaved Analog-to-Digital Converters*. In IEEE International Symposium on Circuits and Systems, ISCAS 2008, pp. 576-579, Seattle USA, 18-21 March 2008.

[17] B. Le Gal, L. Bossuet, D. Dallet. *Mathematical functions based watermaking for IPP*. In IEEE International Conference on Electronics, Circuits and Systems, ICECS 2007, pp. 310-313, Marrakech, Maroco, December 11-14 2007.

[16] B. Le Gal, E. Casseau, L. Bossuet, S. Khan. *HLS design flow for the synthesis of multimode systems under multiple constraints*. In IEEE International Conference on Electronics, Circuits and Systems, ICECS 2007, pp. 314-317, Marrakech, Maroco, December 11-14 2007.

[15] M. Jridi, L. Bossuet, B. Le Gal, D. Dallet. *Mismatch Error Compensation Method for Time-Interleaved A/D Converters*. In 12th Workshop on ADC Modeling and Testing, Iasi, Romania, September 19-21, 2007.

[14] M. Jridi, L. Bossuet, B. Le Gal, D. Dallet. *New Adaptive Calibration Method for Time Interleaved Analog to Digital Converters*. In IEEE International NEWCAS Conference, pp. 932- 935, Montréal, Canada, August 5-8, 2007.

[13] M. Jridi, D. Dallet, G. Monnerie, L. Bossuet. *An Offset and Gain Calibration Method for Time-Interleaved Analog to Digital Converters*. In IEEE International Conference on Electronics, Circuits and Systems, ICECS 2006, pp. 1097-1100, Nice, France, December 10-13 2006.

[12] V. Fresnaud, L. Bossuet, D. Dallet, S. Bernard, J.M. Janik, B. Agnus, Ph. Cauvet, Ph. Gandy. *A Low Cost Alternative Method for Harmonics Estimation in a BIST Context*. IEEE European Tests Symposium, ETS, pp. 193-198, May 2006.

[11] M. Jridi, G. Monnerie, L. Bossuet, D. Dallet. *Two of Time-Interleaved ADC Channel Structure : Analysis and Modeling*. In Proceeding of IEEE Instrumentation and Measurement Technology Conference IMTC 2006, pp. 781-785, Sorrento, Italy, April 24-27 2006.

[10] G. Gogniat, W. Burleson, M. O'Malley, L. Bossuet. *IPSec design through an interdisciplinary approach*. In Proceeding of the IEEE 1st International Workshop on Reconfigurable Computing Education (RC Education), Karlsruhe, Allemagne, 1er mars 2006.

[9] G. Gogniat, W. Burleson, L. Bossuet. *Configurable Computing for High-Security/High-Performance Ambient Systems*. In Embedded Computer Systems : Architectures Modeling, and Simulation, SAMOS V, Samos, Grèce, 18-20 juillet 2005.

[8] L. Bossuet, G. Gogniat, J.L. Philippe. *Generic Design Space Exploration for Reconfigurables Architectures*. In 12th IEEE Reconfigurable Architectures Workshop, RAW 2005, Workshop of IEEE IPDPS 05, Denver, Colorado, USA, 4-5 avril 2005.

[7] L. Bossuet, G. Gogniat, W. Burleson. *Dynamically Configurable Security for SRAM FPGA Bitstreams*. In 11th IEEE Reconfigurable Architectures Workshop, RAW 2004, Workshop of IEEE IPDPS 04, Santa Fé, New Mexico, USA, 26-17 avril 2004.

[6] L. Bossuet, G. Gogniat, J.L. Philippe. *Communication Costs Driven Design Space Exploration for Reconfigurable Architectures*. In the 13th International Conference Field Programmable Logic and Applications, FPL'03, Lisbon, Portugal, September 1-3, 2003.

[5] L. Bossuet, G. Gogniat, J.L. Philippe. *Fast Design Space exploration Method for Reconfigurable Architectures*. In Proceedings of International Conference of Engineering of Reconfigurable Systems and Algorithms, ERSA'03, Las Vegas, Nevada, USA, June 23-26, 2003.

[4] S. Bilavarn, G. Gogniat, J.L. Philippe, L. Bossuet. *Fast Prototyping of Reconfigurable Architectures From a C Program*. In IEEE International Symposium on Circuits and Systems, ISCAS'03, Bangkok, Thailand, 25-28 May, 2003.

[3] L. Bossuet, W. Burleson, G. Gogniat, V. Anand, A. Laffely, J.L. Philippe. *Targeting Tiled Architectures in Design Exploration*. In 10th IEEE Reconfigurable Architectures Workshop, RAW 2003, Workshop of IEEE IPDPS 03, Nice, France, April 22, 2003.

[2] S. Bilavarn, G. Gogniat, J.L. Philippe, L. Bossuet. *Fast Prototyping of Reconfigurable Architectures: An Estimation and Exploration Methodology from System-Level Specifications*. In Eleven ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA 2003), Monterey, California, USA, february 2003.

[1] L. Bossuet, G. Gogniat, J.P. Diguet, J.L. Philippe. *A Modeling Method for Reconfigurable Architectures*. In IEEE International Workshop on System-on-Chip for Real-Time Applications, IWSOC'02, Banff, Canada, July 6-7, 2002.