Maria Méndez Real

PhD student in Electrical and Computer Engineering

Multi/Many-Core Architectures – System Security – Side-Channel Attacks and Countermeasures – Operating Systems

Personal Details

Nationality	Mexican
Date of Birth	13-09-1989
Lab-STICC	Laboratory CNRS UMR 6285 Université Bretagne Sud, BP 92116 - 56321 LORIENT Cedex, FRANCE
Phone number	+33 (0)6 85 48 20 34
E-mail	mendez.real.maria@gmail.com maria.mendez@univ-ubs.fr
web page	`http://www-labsticc.univ-ubs.fr/~mendez`

Education & Qualifications

2014 – 2016 **Laboratoire Lab-STICC, France (2014-2016)**,
Currently in 3rd year of PhD in the frame of the national TSUNAMY project Secure Deployment of Parallel Applications on Many-Core Architectures.

2012 – 2014 **Université de Bretagne-Sud, France (2012-2014)** ,
2-year Master degree I-MARS Microtechnologies Architecture Networks and Communication Systems, with Honours, Ranked: 2^{nd} out of 35.

2009 – 2012 **Université de Bretagne-Sud, France (2012-2014)** ,
Bsc Electrical and Computer Engineering – Embedded Systems, with Honours, Ranked: 1^{st} out of 12.

2009 **Lycée Franco-Mexicain, Mexico (2005-2009)**,
Baccalauréat Scientifique (High School diploma, scientific option), with Honours.

Skills

Programming Languages	C, C++, SystemC Matlab, Scilab VHDL Java Html Latex
Optimization	Metaheuristics Modelling, Simplex Solving Linear Programming Scheduling
FPGA Prototyping	Xilinx(ISE, PlanAhead) Altera(Quartus II)
Operating Systems	Windows, Linux
Modeling	Grafcet, UML, SQL
Multiprocessors Systems-on-Chip	Multi and Many-Core systems, Network-on-Chip, Simulation Tools for Multi and Many-Core Design and Evaluation (OVP, MPSoCSim)
Security	Side-Channel Attacks and Countermeasures

Experience

2015

Ruhr-University Bochum (RUB), in the MCA (Multi-Core Architectures) research group, Germany. October 2015-January 2016,
Invited PhD researcher stay.
Extension of the OVP-based MPSoCSim Simulator for the Virtual Prototyping of Multi/Many-Core Systems
Advisor: Diana Goehringer, Assistant Professor, diana.goehringer@rub.de

2014

Lab-STICC (Centre de Recherche Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance), France. April 2014-August 2014,
Research internship.
Investigation of Resources Allocation Policies on Many-core systems: Application to the TSAR Architecture in a Cryptographic Context
Advisor: Guy Gogniat, Professor, guy.gogniat@univ-ubs.fr

2013

Lab-STICC (Centre de Recherche Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance), France. April 2013-August2013,
Research internship.
Investigation of Power Optimsation Techniques on Networks-on-Chip: Investigation of the Impact of Data on the Network-on-Chip Throughput and Power Consumption
Advisors: André Rossi, Associate Professor, andre.rossi@univ-angers.fr and Johan Laurent Associate Professor, johan.laurent@univ-ubs.fr

2012

Lab-STICC (Centre de Recherche Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance), France. May 2012-July 2012,
Research internship.
Design and Implementation of Image Processing Algorithms
Advisor: Christian Roland, Associate Professor, christian.roland@univ-ubs.fr

Teaching & Lecturing Experience

2014 2016

Analog Electronics,
Lectures, Tutorials and Lab Sessions for 2^{nd} and 3^{rd} year of Electrical and Computer Engineering,
Université de Bretagne-Sud (UBS), France, 2014 - 2016.

2014 2016

Process Automation,
Lectures, Tutorials and Lab sessions for 3^{rd} year of Electrical and Computer Engineering,
Université de Bretagne-Sud (UBS), France, 2014 - 2016.

2014 2016

Technology of Electronic Components,
Lectures, Tutorials and Lab sessions for 3^{rd} year of Electrical and Computer Engineering,
Université de Bretagne-Sud (UBS), France.
2014 - 2016

2014 2016

FPGA Prototyping,
Lab Sessions for 1^{st} year of Master in Electrical and Computer Engineering,
Université de Bretagne-Sud (UBS), France, 2014 - 2016.

2010 2014

Spanish,
Providing Spanish classes to all levels of learners from beginners to advanced,
Association France-Amérique Latine- Alma latina, France, 2010 - 2014.

Internship Supervision

2015

Thomas Toublanc, 2^{nd} of Master in I-MARS Microtechnologies Architecture Networks and Communication Systems at Université de Bretagne-Sud (UBS), France. April 2015-August 2015,
Implementation of a Multiprocessor Platform hosting an Operating System on an FPGA Board.

2015

Esperance Ansgar Djelar, 2^{nd} of Master in I-MARS Microtechnologies Architecture Networks and Communication Systems at Université de Bretagne-Sud (UBS), France. April 2015-August 2015 ,
Comparison of Virtual Platform Simulators: GEM5 and OVPSim.

Publications

Invited Talks

2016 **Investigation on Spatial Isolation against Logical Cache-based Side-Channel Attacks in Multi/Many-Core Architectures**,
Maria Méndez Real, in the final Conference on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE), Barcelona, Spain, 2016.

2016 **Spatial Isolation against Logical Cache-based Side-Channel Attacks on Multi/Many-Core Architectures**,
Maria Méndez Real, at the Séminaire sécurité des systèmes électroniques embarqués, IRISA-DGA, Rennes, France, 2016.

International Journals

2016 **Hardware/Software co-Design of an Accelerator for FV Homomorphic Encryption Scheme using Karatsuba Algorithm**,
Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, in IEEE Transactions on Computers , vol.PP, no.99, pp.1-1.

2016 **Exploration of Application Deployment Strategies for Application Spatial Isolation on Many-core Accelerators against Software Cache-based Side-Channel Attacks**,
Under revision.

International Conferences

2016 **Fast polynomial arithmetic for Somewhat Homomorphic Encryption operations in hardware with Karatsuba algorithm**,
Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, in Proc. of theInternational Conference on Field-Programmable Technology (FPT), Xi'an, China, 2016.

2016 **MPSoCSim extension: An OVP Simulator for the Evaluation of Cluster-based Multicore and Many-Core Architectures**,
Maria Méndez Real, Philipp Wehner, Jens Rettkowski, Vincent Migliore, Vianney Lapotre, Diana Göhringer, Guy Gogniat, in Proc. of the International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (SAMOS XV), Samos, Greece, 2016.

2016 **Dynamic Spatially Isolated Secure Zones for NoC-based Many-core Accelerators**,
Maria Méndez Real, Philipp Wehner, Vincent Migliore, Vianney Lapotre, Diana Göhringer, Guy Gogniat, in Proc. of the 11th International Workshop on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), Tallinn, Estonia, 2016.

2016 **ALMOS many-core operating system extension with new secure-aware mechanisms for dynamic creation of secure zones**,
Maria Méndez Real, Vincent Migliore, Vianney Lapotre, Guy Gogniat, in Proc. of the 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), Crete, Greece, 2016.

2015 **Exploration of Polynomial Multiplication Algorithms for Homomorphic Encryption Schemes**,
Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, in Proc. of the International Conference on Reconfigurable Computing and FPGAs (ReConFig), Cancun, Mexico, 2015.

2015 **Applications security in manycore platform, from operating system to hypervisor: how to build a chain of trust**,
Maria Méndez Real, Vianney Lapotre, Guy Gogniat, Mehdi Aichouch, Moha Ait Hmid, Cuauhtemoc Mancillas López, Lilian Bossuet, Viktor Fischer, in the Workshop on Cryptographic Hardware and Embedded Systems (CHES), Saint Malo, France, 2015 (Poster).

2015 **Exploration of the best polynomial multiplication algorithm for homomorphic encryption schemes**,
Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, in the Workshop on Cryptographic Hardware and Embedded Systems (CHES), Saint Malo, France, 2015 (Poster).

2014 **Trusted computing using enhanced manycore architectures with cryptoprocessors**,
Cuauhtemoc Mancillas Lopez, Maria Méndez Real, Lillian Bossuet, Guy Gogniat, Viktor Fischer, Adel Baganne, in Proc. of the 22nd IFIP/IEEE International Conference on Very Large Scale Integration, (VLSI-SoC), Playa del Carmen, Mexico, 2014.

2014 **Secure deployment in trusted many-core architectures**,
Maria Méndez Real, Guy Gogniat, Adel Baganne, in Proc. of the Women in CAS/ Young Professionals/ MSc/ PhD Forum of the 21st IEEE International Conference on Electronics Circuits and Systems (ICECS), Marseille, France, 2014.

International Workshops

2016 **Dynamic Spatially Isolated Secure zones for NoC-based Multi and Many-core Accelerators** ,
Maria Méndez Real, Vincent Migliore, Vianney Lapotre, Guy Gogniat, in the international workshop on Cryptographic Architectures Embedded in Reconfigurable Devices (CryptArchi), La Grande-Motte, France, 2016.

2016 **On realistic speedup and possible homomorphic operations of Somewhat Homomorphic Encryption Schemes in hardware**,
Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, in the international workshop on Cryptographic Architectures Embedded in Reconfigurable Devices (CryptArchi), La Grande-Motte, France, 2016.

2015 **Special session on the TSUNAMY project**,
Maria Méndez Real, Vianney Lapotre, Guy Gogniat, Mehdi Aichouch, Moha Ait Hmid, Cuauhtemoc Mancillas López, Lilian Bossuet, Viktor Fischer, in the international workshop on Cryptographic Architectures Embedded in Reconfigurable Devices (CryptArchi), Leuven, Belgium, 2015.

2015 **Somewhat homomorphic encryption schemes: which candidates and which expectations to have with this type of encryption schemes?**,
Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, in the international workshop on Cryptographic Architectures Embedded in Reconfigurable Devices (CryptArchi), Leuven, Belgium, 2015.

French Conferences and Workshops

2016 **Algorithmes pour le chiffrement homomorphe**,
Vincent Migliore, Maria Méndez Real, Vianney Lapôtre, Guy Gogniat, in the French Conférence d'informatique en Parallélisme, Architecture et Système (COMPAS), Lorient, France, 2016.

2016 **Déploiement d'applications parallèles sécurisée sur des architectures many-core**,
Maria Méndez Real, Vincent Migliore, Vianney Lapotre, Guy Gogniat, in the French Conférence d'informatique en Parallélisme, Architecture et Système (COMPAS), Lorient, France, 2016.

2015 **Déploiement d'applications parallèles sécurisée sur des architectures many-core**,
Maria Méndez Real, Vincent Migliore, Vianney Lapotre, Guy Gogniat, in the French In the Journées Nationales du Réseau Doctoral en Micro-nanoélectronique (JNRDM), Bordeaux, France, 2015.

2015 **Cryptographie complètement homomorphe : Quels candidats et quelles attentes à avoir pour l'accélération matérielle de ces schémas de chiffrement?**,
Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, in the French In the Journées Nationales du Réseau Doctoral en Micro-nanoélectronique (JNRDM), Bordeaux, France, 2015.

2014 **Secure deployment in trusted many-core architectures**,
Maria Mendez Real, Guy Gogniat, Adel Baganne, in the French Colloque GdR SoC-SiP, Paris, France, 2014.

2014 **Extending Multicore Architectures with Cryptoprocessors and Parallel Cryptography**,
Cuauhtemoc Mancillas Lopez, Maria Méndez Real, Lilian Bossuet, Guy Gogniat, Viktor Fischer, Adel Baganne, in the French Colloque GdR SoC-SiP, Paris, France, 2014.

Reviews in International Conferences

2016 **MCSoC**, IEEE International Symposium on Embedded Multicore/Many-core Systems-on-Chip, 2016.

2016 **ICCS**, International Conference on Computational Science, 2016.

2016 **ALCHEMY Workshop**, Architecture, Languages, Compilation and Hardware support for Emerging ManY-core systems, 2016.

2015 **LASCAS**, IEEE Circuits and Systems society, 2015, 2016.

International Collaborations

Diana Goehringer, Assistant Professor at the Ruhr-University Bochum (RUB), Germany, diana.goehringer@rub.de
Collaboration on multi and many-core simulation tools

Eduardo de la Torre, Associate Professor at Centro de Electronica Industrial (CEIUPM), Madrid, Spain eduardo.delatorre@upm.es
Collaboration on genetic algorithms for mapping strategies on multi-core platforms

Khurram Bhatti, Assistant Professor at the Information Technology University (ITU), Lahore, Pakistan, khurram.bhatti@itu.edu.pk
Collaboration of optimization of mapping algorithms

French Collaborations

LiP6, Laboratoire d'informatique de Paris 6
Virtualization Mechanisms on Many-Core Architectures on the Frame of the French TSUNAMY Project

CEA LIST, Commissariat a l'Energie Atomique et aux Energies Alternatives
Hypervisor on Many-Core Architectures on the Frame of the French TSUNAMY Project

LabHC, Laboratoire Hubert Curien, UMR CNRS 5516, Université Jean Monnet Saint-Etienne
Hardware Cryptoprocessors on the Frame of the French TSUNAMY Project

References

Guy Gogniat, Professor at the Université de Bretagne-Sud (UBS), France, guy.gogniat@univ-ubs.fr
Vianney Lapotre, Associate Professor at the Université de Bretagne-Sud (UBS), France, vianney.lapotre@univ-ubs.fr
Diana Goehringer, Assistant Professor at the Ruhr-University Bochum (RUB), Germany, diana.goehringer@rub.de

Languages

Spanish	Native Speaker
French	Professional Proficiency (2005-Present)
English	Professional Proficiency - 1 year studies in the USA - TOEIC certification–920 points, C level (maximum level) (2015)
German	Basic Communication Skills - A1.1 level certificate (2015)

Honours and Scholarships

2017 **FADEx (French-American Doctoral Exchange)**, Grant for participation to the FADEx program, 2017.

2015 **DAAD (German Academic Exchange Service) Excellence Short-Term Research Grant**, German Grant for a Research Stay in Germany, 2015.

2015 **French UEB (Université Européenne de Bretagne) PhD Exchange Program**, French grant for a research stay in Germany, 2015.

2015 **Trudevice, Cost Action Grant**, Short Term Scientific Mission (STSM) Grant for a Research Stay in Germany, 2015.

2014–2017 **French ANR (Agence National de la Recherche) PhD Scholarship**,
3-year PhD Scholarship in the Frame of the French TSUNAMY Project, France, 2010 - 2014.

2005–2008 **French/Mexican Highschool Excellence Scholarship (LfM-SEP Scholarship)**, 3-year Scholarship Grant, 2006–2008.

Personal Interests

Sports
Zumba, Dancing, Cross-Caf, Running

Manual Art Work
Customization and Restoration Works, Charcoal Drawing, Sewing