MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES

# CURRICULUM VITAE (maximum 4 pages)

| CV date | 09.25.2019 |
|---|---|

## Part A. PERSONAL INFORMATION

| | | | |
|---|---|---|---|
| First and Family name | José Luis Imaña Pascual | | |
| Social Security, Passport, ID number | 05397648P | Age | 53 |
| Researcher numbers | Researcher ID | | |
| | Orcid code | 0000-0002-4220-4111 | |

### A.1. Current position

| | | | | |
|---|---|---|---|---|
| Name of University/Institution | Complutense University of Madrid | | | |
| Department | Computer Architecture and Automation | | | |
| Address and Country | Physics Faculty, Ciudad Universitaria, Plaza de Ciencias, 1. 28040 Madrid | | | |
| Phone number | 913944384 | E-mail | jluimana@ucm.es | |
| Current position | Associate Professor | | From | 11.2.2007 |
| Espec. cód. UNESCO | 3304 | | | |
| Palabras clave | Digital systems, computer arithmetic, finite-field arithmetic, design of cryptographic hardware | | | |

### A.2. Education

| PhD | University | Year |
|---|---|---|
| Physics | Complutense University of Madrid | 2003 |
| | | |

### A.3. JCR articles, h Index, thesis supervised…

Number of six-year periods with Positive Evaluation granted by the "Spanish research Evaluation Commission (CNEAI)": Three. Last period: from 2013-2018.
JCR Q1 publications: 5. JCR Q2 publications: 5.
Citations: 515 Average citations/year (2013-2017): 68
h-index: 8 Source for citations and h-index: Google Scholar

## Part B. CV SUMMARY *(max. 3500 characters, including spaces)*

I received a PhD degree in Physics in 2003 from Complutense University of Madrid. I worked as an electronic design engineer (R&D) at the Madrid Institute of Technology (1991-1993) and as Adjunct Professor at the Computer Science College of Segovia (1993-1995). At Complutense University, I was Adjunct Professor (1995-2006) and non tenured Associate Professor (2006-2007). Since 2007, I have been an Associate Professor (tenured, civil servant) in the Department of Computer Architecture and Automation of Complutense University (UCM). During all these years, I have been teaching more than 20 different BS and MS subjects such as Digital Circuits, Digital Systems Design or Integrated Circuits Design.

As a researcher, I have continuously participated in competitive projects during the last 13 years. I have been guest editor of one Special Issue in a Springer journal (indexed in JCR) and co-editor of a Lecture Notes in Computer Science (LNCS) workshop proceedings. I have co-authored a research book (McGraw-Hill) and I have been author of one book chapter (CRC-Press). I have also authored and co-authored numerous publications in international journals and conferences in the field of design automation of digital systems, including: IEEE Trans. on Computers (2), IEEE Trans. on Industrial Electronics (2), IEEE Trans. on Circuits and Systems I: Regular Papers (2), IEEE Trans. on Circuits and Systems II: Express Briefs (1), IEEE Trans. on VLSI Systems (1), IET Electronics Letters (1), DATE (1), FCCM (1), among others. I have been the promoter and co-founder of the International Workshop on the Arithmetic of Finite Fields (WAIFI), serving as member of the Steering Committee since its foundation. I have also served as General Chair of WAIFI 2007 (Madrid), WAIFI 2008 (Siena) and Publicity Chair of WAIFI 2018 (Bergen). I have been TPC member of international conferences (FPL, IAS, WAIFI, among others) and frequent reviewer in several

relevant international journals and conferences (IEEE Trans. on Computers, IEEE Trans. on Circuits and Systems I, IEEE Trans. on Industrial Electronics, IEEE Trans. on VLSI Systems, IEEE Trans. on parallel and Distributed Systems, Mathematical Reviews, Microprocessors and Microsystems, DATE, DAC, ARITH, etc.). I performed two researching stays at Freiburg University (1997, 1998) funded by competitive grant (DAAD).

With reference to management responsibilities, I have been Head of Departamental Section of Computer Architecture and Automation at Physics Faculty (Complutense University) from 2010 to date, and Director of the Official Master Degree in "New Electronic and Photonics Technologies" (Physics Faculty, UCM) from 2012 to 2014. I have also worked as a referee for the Spanish research agency (ANEP).

**Part C. RELEVANT MERITS**

**C.1. Publications (including books)**

1. **Imaña, J.L.**: "Fast Bit-parallel Binary Multipliers based on Type-I Pentanomials", IEEE Trans. on Computers, 67(6): 898-904 (2018).
IF(JCR-2017): 3.052 (rank: 8/52) ISSN: 0018-9340 doi: 10.1109/TC.2017.2778730

2. **Imaña, J.L.**: "Reconfigurable implementation of GF($2^m$) bit-parallel multipliers", Design, Automation and Test in Europe & Exhibition (DATE). Dresden (Germany), 2018, pp. 899-902.
CGS Conference Rating: A ISBN: 978-3-9819263-1-6 doi: 10.23919/DATE.2018.8342134

3. **Imaña, J.L.**: "Low-delay AES polynomial basis multiplier", IET Electronics Letters, 52(11): 930-932 (2016).
IF(JCR-2016): 1.155 (rank: 179/262) ISSN: 0013-5194 doi: 10.1049/el.2016.0577

4. **Imaña, J.L.**: "High-Speed Polynomial Basis Multipliers Over GF($2^m$) for Special Pentanomials", IEEE Trans. on Circuits and Systems I: Regular Papers, 63(1): 58-69 (2016).
IF(JCR-2016): 2.407 (rank: 93/262) ISSN: 1549-8328 doi: 10.1109/TCSI.2015.2500419

5. **Imaña, J.L.**, Hermida, R., Tirado, F.: "Low Complexity Bit-parallel Polynomial Basis Multipliers Over Binary Fields for Special Irreducible Pentanomials", INTEGRATION, the VLSI Journal, 46(2), pp. 197-210 (2013).
IF(JCR-2013): 0.529 (rank: 39/50) ISSN: 0167-9260 doi: 10.1016/j.vlsi.2011.12.006

6. Sutter, G.D., Deschamps, J.-P., **Imaña, J.L.**: "Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations", IEEE Trans. on Industrial Electronics, 60(1), pp. 217-225 (2013).
IF(JCR-2013): 6.500 (rank: 2/248) ISSN: 0278-0046 doi: 10.1109/TIE.2012.2186104

7. **Imaña, J.L.**: "Efficient Polynomial Basis Multipliers for Type-II Irreducible Pentanomials", IEEE Trans. on Circuits and Systems II: Express Briefs, 59(11), pp. 795-799 (2012).
IF(JCR-2012): 1.327 (rank: 96/243) ISSN: 1549-7747 doi: 10.1109/TCSII.2012.2222836

8. Sutter, G.D., Deschamps, J.-P., **Imaña, J.L.**: "Modular Multiplication and Exponentiation Architectures for Fast RSA Cryptosystem Based on Digit Serial Computation", IEEE Trans. on Industrial Electronics, 58(7), pp. 3101-3109 (2011).
IF(JCR-2011): 5.160 (rank: 4/245) ISSN: 0278-0046 doi: 10.1109/TIE.2010.2080653

9. **Imaña, J.L.**: "Low Latency GF($2^m$) Polynomial Basis Multiplier", IEEE Trans. on Circuits and Systems I: Regular Papers, 58(5): 935-946 (2011).
IF(JCR-2011): 1.970 (rank: 52/245) ISSN: 1549-8328 doi: 10.1109/TCSI.2010.2089553

10. Deschamps, J-.P., **Imaña, J.L.**, Sutter, G.: "Hardware Implementation of Finite-Field Arithmetic", Ed. McGraw-Hill, 2009.
ISBN: 978-0-07-154581-5

**C.2. Research projects and grants**

1. Title: Efficient heterogeneous computing: from the processor to the datacenter (COPHERNICO)
Funding entity: MINECO (TIN2015-65277-R)
Principal Investigator: Manuel Prieto Matías / Luis Piñuel Moreno
Participating entities: Complutense University of Madrid
Starting date: 01.01.2016 Ending date: 12.31.2018
Role: Investigator
Project amount: 371,470 euros

2. Title: Emerging Architectures and Technologies. Energy Efficiency through heterogeneity (ARTE)
Funding entity: MINECO (TIN2012-32180)
Principal Investigator: Manuel Prieto Matías
Participating entities: Complutense University of Madrid
Starting date: 01.01.2013 Ending date: 12.31.2015
Role: Investigator
Project amount: 219,620 euros

3. Title: Hardware/software architecture for high-performance systems II
Funding entity: National Science Agency (TIN2008-00508)
Principal Investigator: Francisco Tirado Fernández
Participating entities: Complutense University of Madrid
Starting date: 01.01.2009 Ending date: 06.30.2015
Role: Investigator
Project amount: 1,217,260 euros

4. Title: Hardware/software architecture for high-performance systems
Funding entity: National Science Agency (TIN2005-05619)
Principal Investigator: Francisco Tirado Fernández
Participating entities: Complutense University of Madrid
Starting date: 12.31.2005 Ending date: 12.30.2008
Role: Investigator
Project amount: 596,190 euros

5. Title: International Workshop on the Arithmetic of Finite Fields (WAIFI 2007)
Funding entity: National Science Agency – Complementary Action (TIN2006-28228-E)
Principal Investigator: José Luis Imaña Pascual
Participating entities: Complutense University of Madrid
Starting date: 03.30.2007 Ending date: 03.30.2008
Role: PI
Project amount: 3,000 euros

**C.3. Researching Stays**

Institut für Informatik, Albert-Ludwigs University (Freiburg i.B., Germany), PhD researcher, from 07.01.1997 to 09.01.1997.

Institut für Informatik, Albert-Ludwigs University (Freiburg i.B., Germany), PhD researcher, from 08.01.1998 to 02.01.1999.

**C.4. Grants**

Deutscher Akademischer Austauschdienst (DAAD), for stay at Albert-Ludwigs University.

Complutense University grant, for the organization of WAIFI 2007.

**C.5. Collaborations in journals and conferences**

Steering Committee of the International Workshop on the Arithmetic of Finite Fields (WAIFI), period 2007-to date.

General co-Chair of WAIFI 2007 (Madrid) and WAIFI 2008 (Siena, Italy).

Publicity Chair of WAIFI 2018 (Bergen, Norway).

Program Committee of FPL (2007-2012, 2014), WAIFI (2010, 2012), CERMA (2006-2009), ANDESCON (2006), CISIS (2009-2017), IAS (2012-2014).

Session Chair at MixVLSI95, WAIFI 2008, WAIFI 2018.

Reviewer of DATE, DAC, ARC, ICPADS, ICCES, CODES+ISSS, CITSA, CCCT, CISCI, SCI, ARITH (in several editions).

Reviewer of IEEE Trans. on Computers; IEEE Trans. on Circuits and Systems I; IEEE Trans. on Industrial Electronics; IEEE Trans. on VLSI Systems; IEEE Trans. on Parallel and Distributed Systems; IEEE Computer; Microprocessors and Microsystems; INTEGRATION; Intl. Journal on Computers and Electrical Engineering; Journal of Systems Architecture; Journal of The Institution of Engineers (India): Series B; Intl. Journal of Reconfigurable Computing; Journal of Circuits, Systems, and Computers; Mathematical Reviews.

**C.6. Other**

Translation of 3 technical books from English to Spanish (McGraw-Hill).