

**CURRICULUM VITAE**  
**Dr. PARIS KITSOS**

**May 2013**

## **1. PERSONAL DATA**

Name: Paraskevas (Paris) Kitsos  
Birthday: 12 February 1975  
Occupation: Ph.D., Physics degree  
Place of birth: Athens  
Nationality: Greek  
Marital status: Married with one daughter  
Office address: Digital Systems & Media Computing Laboratory,  
School of Science & Technology,  
Hellenic Open University (HOU), Patras, Greece  
Office phone: +30 2610 367535  
Office fax: +30 2610 367528  
E-mail: pkitsos@eap.gr, pkitsos@ieee.org

## **2. BRIEF CURRICULUM VITAE**

In 1993 he joined the Physics Department of the University of Patras, from which he graduated in September 1999. His diploma thesis entitled: “*Digital Systems Processing with the SIMULINK of MATLAB*” was carried out at the Electronics Laboratory, Electronics and Computers Division, Department of Physics, University of Patras under the supervision of Associate professor Spiros Fotopoulos.

From February 2000 until the April 2004 he was pursued his Ph.D. thesis entitled “*Efficient VLSI Implementation of Cryptographic Algorithms and Security Systems for Wireless Communications*”, which was completed with “Excellent” grade. The thesis was carried out at the VLSI Design Laboratory of the Electrical and Computer Engineering Department of the University of Patras.

He has been working with Dr Joan Daemen, STMicroelectronics for the creations of the new cryptography algorithms. They have created the *Self-synchronizing stream ciphers Mosquito* and *Moustique*. These algorithms had been submitted in the eSTREAM, the ECRYPT Stream Cipher Project (European Network of Excellence for Cryptology), project (publications C24 and C29).

From May 2005, which finished his military services, he is working at the Digital Systems & Media Computing Laboratory, School of Science & Technology, Hellenic Open University (HOU), Patras, Greece.

He was Track Co-chair in “*The 4th International Conference on ReConFigurable Computing and FPGA’s, ReConFig’ 08*” (Mexico), also he was *General Local Chair* in “*12th Euromicro Conference on Digital System Design, Architectures, Methods and Tools – DSD 2009*”, (Patras-Greece, August 2009), he was *Deputy Program Chair* in “*13th Euromicro Conference on Digital System Design, Architectures, Methods and Tools – DSD 2010*”, (Lille-France, September 2010), and finally, he was *Program Chairman* in “*14th Euromicro Conference on Digital System Design, Architectures, Methods and Tools – DSD 2011*”, (Oulu-Finland, August - September 2011).

In addition he was Co-editor to the following books: “*RFID Security: Techniques, Protocols and System-On-Chip Design*”, Springer-USA, 2008 and “*Security in RFID and Wireless Sensor Networks*”, Auerbach Publications, 2009.

### **3. EDUCATION**

2/2000 - 4/2004     **Ph.D.**, VLSI Design Laboratory, Department of Electrical and Computer Engineering, University of Patras, Greece.

10/1993 - 9/1999     **Physics Degree**, University of Patras, Greece.

### **4. POSITIONS HELD**

- Research fellow in Digital Systems & Media Computing Laboratory, School of Science & Technology, Hellenic Open University (HOU), Patras, Greece. From 6/2005 to today.

### **5. RESEARCH INTERESTS**

- Hardware Trojans Detection Techniques
- Hardware architectures and implementations of cryptographic algorithms (private-key and public-key algorithms).
- Efficient architectures and implementations for RFID and Lightweight crypto systems.
- Security systems for wireless communications.
- Efficient polynomial basis Galois field arithmetic.
- VLSI design.
- Computer architecture.

### **6. TEACHING EXPERIENCE**

#### ***2012-2013***

- Adjunct Assistant Professor with Telecommunication Systems and Networks, Highest Technological Educational Institute (ATEI) of Messolonghi for the academic year 2012-2013: Tutorships: “Digital Design”, “Computer Architecture”, “Network Security” and “Hardware Description Languages”.

#### ***2011-2012***

- Adjunct Assistant Professor with Telecommunication Systems and Networks, Highest Technological Educational Institute (ATEI) of Messolonghi for the academic year 2011-2012: Tutorships: “Digital Design”, “Computer Architecture”, “Network Security” and “Hardware Description Languages”.
- Adjunct Assistant Professor with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2011-2012: Tutorship: “Multimedia Development”.

#### ***2010-2011***

- Adjunct Assistant Professor with Telecommunication Systems and Networks, Highest Technological Educational Institute (ATEI) of Messolonghi for the academic year 2010-2011: Tutorships: “Digital Design”, “Computer Architecture”, “Network Security” and “Hardware Description Languages”.

- Adjunct Assistant Professor with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2010-2011: Tutorship: “Multimedia Development”.
- Adjunct Assistant Professor in the Department of Computer Engineering and Informatics of the University of Patras for the academic year 2010-2011: Tutorship: Full responsibility for teaching the course “Programming in Symbolic Language (Assembly)”.

#### **2009-2010**

- Adjunct Lecturer in the Department of Computer Science and Technology, University of Peloponnese, for the academic years 2009-2010. Tutorship: Full responsibility for teaching the courses “Hardware Description Languages II” and “Computer Arithmetic” and “Digital Architecture Synthesis”.
- Adjunct Assistant Professor with Telecommunication Systems and Networks, Highest Technological Educational Institute (ATEI) of Messolonghi for the academic year 2009-2010: Tutorships: “Digital Design”, “Network Security”, and “Labs of Hardware Description Languages”.
- Adjunct Assistant Professor with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2009-2010: Tutorships: “Multimedia Development” and “Multimedia Production”.

#### **2008-2009**

- Adjunct Lecturer in the Department of Computer Science and Technology, University of Peloponnese, for the academic years 2008-2009. Tutorship: Full responsibility for teaching the courses “VLSI Design” and “Digital Architecture Synthesis”.
- Adjunct Assistant Professor with Telecommunication Systems and Networks, Highest Technological Educational Institute (ATEI) of Messolonghi for the academic year 2008-2009: Tutorships: “Computer Architecture” and “Network Security”.
- Adjunct Assistant Professor with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2008-2009: Tutorships: “Creative Multimedia Design” and “Multimedia Production”.
- Adjunct Lecturer with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2008-2009: Tutorship: “Educational Multimedia Programs Labs”.

#### **2007-2008**

- Adjunct Lecturer in the Department of Computer Science and Technology, University of Peloponnese, for the academic years 2007-2008. Tutorship: Full responsibility for teaching the courses “VLSI Design” and “FPGA Design and implementation”.
- Adjunct Assistant Professor in the Department of Computer Engineering and Informatics of the University of Patras for the academic year 2007-2008: Tutorship: Full responsibility for teaching the courses “Computer Architecture I” and “Computer Architecture Labs”.
- Adjunct Assistant Professor with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2007-2008: Tutorships: “Creative Multimedia Design” and “Multimedia Production”.
- Adjunct Lecturer with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2007-2008: Tutorship: “Educational Multimedia Programs Labs”.

### **2006-2007**

- Adjunct Assistant Professor in the Department of Computer Engineering and Informatics of the University of Patras for the academic year 2005-2006: Tutorship: Full responsibility for teaching the course “Computer Architecture Labs”.
- Adjunct Lecturer with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2005-2006: Tutorship: “Educational Multimedia Programs Labs”.
- Adjunct Lecturer with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2005-2006: Tutorship: “WEB Design Labs”.

### **2005-2006**

- Adjunct lecturer in the Department of Telecommunications Science and Technology, University of Peloponnese, for the academic years 2005-2006. Tutorship: Full responsibility for teaching the course “Cryptology - Cryptography & Cryptanalysis” (6<sup>th</sup> Semester).
- Adjunct lecturer with Hellenic Open University (HOU) in the thematic unit of *Labs on Digital System* for the academic years 2005-2006.
- Adjunct Assistant Professor with Applied Informatics & Mass Media, Highest Technological Educational Institute (ATEI) of Patras for the academic year 2005-2006: Tutorship: Full responsibility for teaching the course “WEB Design”.

### **2000-2004**

During his Ph.D he was teaching assistant in several laboratorial courses. In more details.

- Teaching Assistant, Electrical & Computer Engineering Dept., University of Patras, Greece, Undergraduate Laboratory: “Introduction to Computers II”, 1<sup>st</sup> semester, 2000-2004.
- Teaching Assistant, Electrical & Computer Engineering Dept., University of Patras, Greece, Undergraduate Laboratory: “Introduction to Computers I”, 2<sup>st</sup> semester, 2001-2004.
- Teaching Assistant, Electrical & Computer Engineering Dept., University of Patras, Greece, Undergraduate Laboratory: “VLSI Design I”, 7<sup>th</sup> semester, 2001-2004.
- Teaching Assistant, Electrical & Computer Engineering Dept., University of Patras, Greece, Undergraduate Laboratory: “VLSI Design II”, 8<sup>th</sup> semester, 2000-2004.
- Supervision of 5 Completed Diploma Thesis, on Design and Implementation of Cryptography Algorithms, Security Systems for Wireless Protocols, Design for Low Power VLSI Circuits.

## **7. CONTRIBUTION TO RESEARCH PROJECTS**

- A. Management committee member of the COST ACTION IC1204 “**Trustworthy Manufacturing and Utilization of Secure Devices**”.
- B. Research project: “**Services and Infrastructures in Future Internet**”. Research and developmental project with Technological Educational Institute of Messolonghi.
- C. Research project: “**Designing a Structured Architecture of Hardware and Software of Sensors Network Nodes – ModSense**”. Research and developmental project with Industrial Systems Institute (ISI).
- D. Research project: “**STREP VITAL: Enabling convergence of IP multimedia services over next generation networks technology**”. Research and developmental project with European Union.
- E. Research project: “**Provision System of Interaction Services**”. Research and developmental project with Regional Development Fund of the Region of Western Greece.
- F. **Educational Program of Hellenic Open University**, growth of instructive material – program of study of thematic unit with subjects of *Advanced Topics of Computer Networks, Digital*

*Communications, Cryptography and Networks Security* which belongs in the postgraduate program of study “**Postgraduate Specialization in the Informative Systems**” of the Hellenic Open University.

- G. Research project: “**FLEXINET – Design and Development of Generic Application Interface Bus**”. Research and development project with Department of Electrical and Computer Engineering, VLSI Design Laboratory, University of Patras cooperation.
- H. Research project: “**Low Power Bluetooth System**”. Research and developmental project with ATMEL HELLAS cooperation.
- I. Research project: “**Cryptography Algorithms Development and Implementation**”. Research project with Hellenic Aerospace Industry cooperation.
- J. Research project with International, Communications of Greece (OTE). “**Research Project on Wireless communications of DECT in the future communications systems/protocols of OTE (OTE-Hellenic Telecommunication Organization)**”.

## **8. SOCIETIES MEMBERSHIP**

- Member of Greek Scientific Union for the evaluation of research and technological work proposals that is submitted in the frame of National Programs. General Secretariat of Research and Technology.
- Institute of Electrical and Electronics Engineers (IEEE).

## **9. COLLABORATIONS**

### **• NATIONAL**

- 1) Prof. Athanassios N. Skodras, University of Patras, Electrical and Computer Engineering Department.
- 2) Prof. Odysseas Koufopavlou, University of Patras, Electrical and Computer Engineering Department, VLSI Design Laboratory.

### **• INTERNATIONAL**

1. Dr. Joan Daemen, STMicroelectronics Belgium.
2. René Cumplido, National Institute for Astrophysics Optics and Electronics, Mexico.
3. Dr. Akashi Satoh, National Institute of Advanced Industrial Science and Technology (AIST), Tokyo.

## **10. COMPUTER SKILLS**

- CAD tools for VLSI design: Mentor Graphics, Synopsis.
- CAD tools for FPGA design: LeonardoSpectrum, Xilinx ISE, Xilinx Foundation Software.
- Hardware Description Language: VHDL.
- Programming languages: FORTRAN.
- Mathematical software: Simulink - MATLAB.
- Programs of Automation Office: MS OFFICE, OPEN-OFFICE and VISIO PROFESSIONAL.
- Operating systems: WINDOWS, UNIX.

## **11. LANGUAGES**

- English.
- Greek (native).

## **12. PUBLICATIONS**

### **I. Books**

- B4. Nicolas Sklavos, Michael Huebner, Diana Goehringer, Paris Kitsos, “System-Level Design Methodologies for Telecommunication”, Springer-USA, 2013.
- B3. Paris Kitsos, “Digital System Design: Architectures, Methods and Tools”, 14th EUROMICRO Conference on Digital System Design (DSD), Oulu, Finland, August 31st - September 2nd, 2011, Proceedings. Published by the IEEE Computer Society, ISBN 978-0-7695-4494-6.
- B2. Y. Zhang and P. Kitsos (Editors), “Security in RFID and Sensor Networks”, Auerbach Publications, ISBN-10: 1420068393, ISBN-13: 978-1420068399, 2009.
- B1. P. Kitsos and Y. Zhang (Editors), “RFID Security: Techniques, Protocols and System-On-Chip Design”, Springer-USA, ISBN-10: 0387764801, ISBN-13: 978-0387764801, 2008.

### **II. Book Chapters**

- BC6. A. P. Fournaris, P. Kitsos and N. Sklavos, “Security and Cryptographic Engineering in Embedded Systems”, *Embedded Computing Systems: Applications, Optimization, and Advanced Design*, IGI Global, ISBN13: 9781466639225, 2013.
- BC5. G. Kalogeridou, N. Sklavos, P. Kitsos, “System Design and FPGA Implementation for a Cognitive Radio Wireless Device”, Chapter in the book *Cognitive Radio and its Technological Impact on Wireless Cellular and Vehicular Networks*, Series Lectures Notes in Electrical Engineering, Vol. 116, Springer, ISBN: 978-94-007-1826-5, 2012.
- BC4. Joan Daemen and Paris Kitsos, “The Self-Synchronizing Stream Cipher Moustique”, Chapter in the book *The eStream Finalists*, Lecture Notes in Computer Science, Volume 4986/2008, ISBN: 978-3-540-68350, Springer, 2008.
- BC3. Giorgos Kostopoulos, Paris Kitsos and Odysseas Koufopavlou, “Mobile Pervasive Computing Security Implementations: The Bluetooth Example”, *Chapter in the book The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*, Auerbach Publications, Taylor&Francis Group, ISBN: 1420052810, USA, February, 2008.
- BC2. Paris Kitsos, “System-on-chip Design of the Whirlpool Hash Function”, chapter in the book *Handbook of Research on Wireless Security*, Idea Group Inc., ISBN-10: 159904899X, 2007.
- BC1. Paris Kitsos and Nikos Sklavos, “Security Architecture and Implementation of the Universal Mobile Telecommunication System (UMTS)”, chapter in the book *Handbook of Wireless Security: From Specifications to Implementations*, CRC-Press, ISBN: 9780849387715, 2007.

### **III. Journal publications**

- J17. Morales-Sandoval, C. Feregrino-Uribe, R. Cumplido, P. Kitsos, “Area/performance trade-off analysis of an FPGA digit-serial GF(2<sup>m</sup>) Montgomery Multiplier based on LFSR”, *Computer and Electrical Engineering*, Elsevier, 2013. (Included in ISI/SCI)
- J16. Paris Kitsos, Nicolas Sklavos, George Provelengios, Athanassios Skodras, “FPGA-based Performance Analysis of Stream Ciphers ZUC, Snow3g, Grain v1, Mickey v2, Trivium and E0”, *Microprocessors and Microsystems: Embedded Hardware Design* (accepted), 2013. (Included in ISI/SCI)

- J15.P. Kitsos, N. Sklavos, M. Parousi, A. N. Skodras, "A Comparative Study of Hardware Architectures for Lightweight Block Ciphers", *Computer and Electrical Engineering* - Elsevier, vol. 38, no. 1, pp. 148-160, 2012. (Included in ISI/SCI)
- J14.M. Morales-Sandoval, C. Feregrino-Uribe, P. Kitsos, "Bit-Serial and Digit-Serial GF(2<sup>m</sup>) Montgomery Multipliers using Linear Feedback Shift Registers", *IET Computers & Digital Techniques*, Vol. 5, Issue. 2, March 2011. (Included in ISI/SCI)
- J13.P. Kitsos, N. Sklavos, and O. Koufopavlou, "UMTS Security: System Architecture and Hardware Implementation", *Wireless Communications and Mobile Computing Journal*, Volume 7, Issue 4, May 2007. (Included in ISI/SCI)
- J12.P. Kitsos, "Hardware Implementations for the ISO/IEC 18033-4:2005 Standard for Stream Ciphers", *International Journal of Signal Processing (IJSP)*, Vol: 3, No. 2, 2007.
- J11.P. Kitsos, M. D. Galanis, and O. Koufopavlou, "Architectures and FPGA Implementations of the 64-bit MISTY1 Block Cipher", *World Scientific Journal of Circuits, Systems, and Computers (JCSC)*, Vol. 15, No. 6, December 2006. (Included in ISI/SCI)
- J10.N. Sklavos, P. Kitsos, K. Papadopoulos and O. Koufopavlou, "Design, Architecture and Performance Evaluation of the Wireless Transport Layer Security (WTLS)", *Journal of Supercomputing*, Kluwer Academic Publishers, Volume 36, No. 1, pp: 33-50, 2006. (Included in ISI/SCI)
- J9. M. D. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, and C. E. Goutis, "Comparison of the Hardware Implementation of Stream Ciphers", *The International Arab Journal of Information Technology (IAJIT)*, Colleges of Computer and Information Society, Vol. 2, No. 4, October 2005, pp. 267-274. (Included in ISI/SCI)
- J8. P. Kitsos, M. D. Galanis, and O. Koufopavlou, "An FPGA Implementation of the GPRS Encryption Algorithm 3 (GEA3)", *Journal of Circuits, Systems, and Computers (JCSC)*, World Scientific Publishing Company, Vol. 14, No. 2, pp: 217-231, 2005. (Included in ISI/SCI)
- J7. P. Kitsos, O. Koufopavlou, G. Selimis, and N. Sklavos, "Low Power Cryptography", (selected to be published from Microelectronics, Microsystems and Nanotechnology: MMN'04), *Journal of Physics: Conferences series, IoP Journals*, Vol. 10, pp: 343-347, 2005.
- J6. N. Sklavos, P. Kitsos, E. Alexopoulos, and O. Koufopavlou, "Open Mobile Alliance (OMA) Security Layer: Architecture Implementation and Performance Evaluation of the Integrity Unit", *New Generation Computing: Computing Paradigms and Computational Intelligence*, Springer-Verlag, Vol. 23, No 1, pp. 77-100, 2005. (Included in ISI/SCI)
- J5. P. Kitsos, N. Sklavos, M. D. Galanis, and O. Koufopavlou, "64-bit Block Ciphers: Hardware Implementation and Comparison Analysis", *Computers and Electrical Engineering*, Elsevier Science, Vol. 30, Issue: 8, pp. 593-604, November 2004. (Included in ISI/SCI)
- J4. P. Kitsos and O. Koufopavlou, "Efficient Architecture and Hardware Implementation of the Whirlpool Hash Function", *IEEE Transactions on Consumer Electronics*, Vol. 50, Issue 1, February 2004, pp. 208-213. (Included in ISI/SCI)
- J3. P. Kitsos and O. Koufopavlou, "Configurable Hardware Implementations of Bulk Encryption Units for Wireless Communications", *The International Arab Journal of Information Technology (IAJIT)*, Colleges of Computer and Information Society, Vol. 1, No. 1, January 2004, pp. 122-126. (Included in ISI/SCI)
- J2. P. Kitsos, G. Theodoridis, and O. Koufopavlou, "An Efficient Reconfigurable Multiplier Architecture for Galois field GF(2<sup>m</sup>)", *Elsevier Microelectronics Journal*, Vol. 34, Issue 10, October 2003, pp. 975-980. (Included in ISI/SCI)



- J1. P. Kitsos, N. Sklavos, K. Papadomanolakis and O. Koufopavlou, "Hardware Implementation of the Bluetooth Security", *IEEE Pervasive Computing, Mobile and Ubiquitous Systems*, Vol. 2, No. 1, Jan.-Mar. 2003, pp. 21-29. (Included in ISI/SCI)

#### **IV. Publications in conference/workshops proceedings**

- C40. Paris Kitsos, Nikolaos S. Voros, Tasos Dagiuklas, Athanassios N. Skodras, "A High Speed FPGA Implementation of the 2D DCT for Ultra High Definition Video Coding", 18th International Conference on Digital Signal Processing (DSP 2013), Island of Santorini, Greece, July 1-3, 2013.
- C39. G. Provelengios, P. Kitsos, N. Sklavos, C. Koulamas, "FPGA-based Design Approaches of Keccak Hash Function", 15th Euromicro Conference on Digital Systems (DSD'12), Izmir, Turkey, 5-8 September, 2012.
- C38. N. Sklavos, P. Kitsos, O. Koufopavlou, "VLSI Design and Implementation of Homophonic Security System", IEEE Computer Society Annual Symposium on VLSI (ISVLSI), University of Massachusetts, Amherst, USA, August 19-21, 2012.
- C37. N. Sklavos, P. Kitsos, "Architectural Optimizations & Hardware Implementations of WLANs Encryption Standard", 5th International Conference on New Technologies, Mobility and Security (NTMS'12), Istanbul, Turkey, May 7-10, 2012.
- C36. P. Kitsos, N. Sklavos and A. N. Skodras, "A FPGA Implementation of the ZUC Stream Cipher", 14th Euromicro Conference on Digital Systems (DSD'11), Oulu, Finland, August 31 - September 2, 2011.
- C35. G. Provelengios, N. Voros and P. Kitsos, "Low Power FPGA Implementations of JH and Fugue Hash Functions", 14th Euromicro Conference on Digital Systems (DSD'11), Oulu, Finland, August 31 - September 2, 2011.
- C34. P. Kitsos and A. N. Skodras, "An FPGA Implementation and Performance Evaluation of the Seed Block Cipher", 17th Int. Conference on Digital Signal Processing (DSP'11), Corfu, Greece, 6-8 July 2011.
- C33 P. Kitsos, N. Sklavos, "On the Hardware Implementation Efficiency of SHA-3 Candidates", 17th IEEE International Conference on Electronics, Circuits, and Systems, (ICECS'10), December 12-15, Athens, Greece, 2010.
- C32 Paris Kitsos, Nicolas Sklavos, Athanassios N. Skodras, "Low Power FPGA Implementations of 256-bit Luffa Hash Function", 13th Euromicro Conference on Digital Systems (DSD'10), Lille, France, September 1-3, 2010.
- C31 Nicolas Sklavos and Paris Kitsos, "BLAKE HASH Function Family on FPGA: From the Fastest to the Smallest", IEEE Computer Society Annual Symposium on VLSI (IEEE ISVLSI'10), Kefalonia, Greece, July 5-7, 2010.
- C30 P. Kitsos, G. Selimis, O. Koufopavlou, "High Performance ASIC Implementation of the SNOW 3G Stream Cipher", *IFIP/IEEE VLSI-SOC 2008 - International Conference on Very Large Scale Integration (VLSI SOC)*, Rhodes Island, Greece, October 13-15, 2008.
- C29 P. Kitsos, G. Selimis, O. Koufopavlou, A. N. Skodras, "A Hardware Implementation of CURUPIRA Block Cipher for Wireless Sensors", *11th Euromicro Conference on Digital System Design, Architectures, Methods and Tools, DSD 2008*, Parma Italy, 3 - 5 September, 2008.
- C28 Paris Kitsos and Ulrich Kaiser, "A High-Speed Hardware Implementation of the Hermes8-128 Stream Cipher", *18th European Conference on Circuit Theory and Design 2007 - ECCTD 2007*, August 26- 30, 2007, Seville, Spain.
- C27 Paris Kitsos and Odysseas Koufopavlou, "An FPGA-Based Implementation of the Pomaranch Stream Cipher", *3rd International Mobile Multimedia Communications Conference (MSAN) - MobiMedia 2007*, August 27-29, 2007, Nafpaktos, Greece.

- C26 Paris Kitsos and Bhanu Prasad, "A System-on-Chip Design of the RadioGatún Hash Function", *International Conference on High Performance Computing, Networking and Communication Systems*, 9-12 of July 2007 in Orlando, FL, USA.
- C25 J. Daemen and P. Kitsos, "The self-synchronizing stream cipher Moustique", *eSTREAM Phase 2, the ECRYPT Stream Cipher Project, (ECRYPT NoE)*. August 2006.
- C24 P. Kitsos and A. N. Skodras, "On the Hardware Implementation of the MUGI Pseudorandom Number Generator", In proc. *of the Fifth International Symposium on Communications Systems, Networks and Digital Signal Processing, (CSNDSP'2006)*, Patras, Greece, 19-21 July, 2006.
- C23 P. Kitsos, N. Sklavos and O. Koufopavlou, "A High-Speed Hardware Implementation of the LILI-II Keystream Generator", In proc. *of the Fifth International Symposium on Communications Systems, Networks and Digital Signal Processing, (CSNDSP'2006)*, Patras, Greece, 19-21 July, 2006.
- C22 J. Daemen and P. Kitsos, "The self-synchronizing stream cipher Mosquito", *eSTREAM Phase 1, the ECRYPT Stream Cipher Project, (ECRYPT NoE)*, Scandinavian Congress Center, Aarhus, Denmark, 26-27 May 2005. This paper also has been presented in *Symmetric Key Encryption Workshop (SKEW)*, Scandinavian Congress Center, Aarhus, Denmark, 26-27 May 2005.
- C21 P. Kitsos, M. D. Galanis, and O. Koufopavlou, "A RAM-Based FPGA Implementation of the 64-bit MISTY1 Block Cipher", In proc. *of IEEE International Symposium on Circuits & Systems (ISCAS'05)*, Kobe, Japan, May 23-26, 2005.
- C20 M. D. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, O. Koufopavlou, and C. E. Goutis, "Comparison of the Hardware Architectures and FPGA Implementations of Stream Ciphers", In proc. *of 11th IEEE International Conference on Electronics, Circuits and Systems, (ICECS 2004)*, Tel-Aviv, Israel, December 13-15, 2004.
- C19 G. Selimis, P. Kitsos and O. Koufopavlou, "High Performance Cryptographic Engine PANAMA: Hardware Implementation", In proc. *of 11th IEEE International Conference on Electronics, Circuits and Systems, (ICECS 2004)*, Tel-Aviv, Israel, December 13-15, 2004.
- C18 M. D. Galanis, P. Kitsos, G. Kostopoulos and O. Koufopavlou, "Comparison of the Performance of Stream Ciphers for Wireless Communications", In proc. *of International Conference on Computing, Communications and Control Technologies 2004 (CCCT'04)*, Austin, Texas, USA, August 14-17, 2004.
- C17 P. Kitsos, N. Sklavos, M. D. Galanis and O. Koufopavlou, "An FPGA-Based Performance Comparison of the 64-bit Block Ciphers", In proc. *of World Automation Congress 2004 (WAC 2004)*, Spain, Seville, June 28-July 1, 2004.
- C16 P. Kitsos, M. D. Galanis and O. Koufopavlou, "High-Speed Hardware Implementations of the KASUMI Block Cipher", In proc. *of IEEE International Symposium on Circuits & Systems (ISCAS'04)*, Canada, May 23-26, 2004.
- C15 P. Kitsos and O. Koufopavlou, "Whirlpool Hash Function: Architecture and VLSI Implementation", In proc. *of IEEE International Symposium on Circuits & Systems (ISCAS'04)*, Canada, May 23-26, 2004.
- C14 P. Kitsos and O. Koufopavlou, "A Reconfigurable Most/Least Significant Bit Multiplier for  $GF(2^m)$ ", In proc. *of IEEE Workshop on Wireless Circuits and Systems (WoWCAS 2004)*, Canada, May 21-22, 2004.
- C13 P. Kitsos, N. Sklavos, and O. Koufopavlou, "An End-to-End Hardware Approach Security for the GPRS", In proc. *of The 12th IEEE Mediterranean Electrotechnical Conference - MELECON 2004*, Croatia, Dubrovnic, May 12-15, 2004.

- C12 P. Kitsos and O. Koufopavlou, "A Time and Area Efficient Hardware Implementation of the MISTY1 Block Cipher", In proc. of *46th IEEE Midwest Symposium on Circuits & Systems '03*, December 27-30, Cairo, Egypt, 2003.
- C11 P. Kitsos, G. Kostopoulos, N. Sklavos and O. Koufopavlou, "Hardware Implementation of the RC4 stream Cipher", In proc. of *46th IEEE Midwest Symposium on Circuits & Systems '03*, December 27-30, Cairo, Egypt, 2003.
- C10 N. Sklavos, A. Priftis, P. Kitsos and O. Koufopavlou, "Reconfigurable Crypto-Processor Design of Encryption Algorithms Operation Modes: Methods and FPGA Integration", In proc. of *46th IEEE Midwest Symposium on Circuits & Systems '03*, December 27-30, Cairo, Egypt, 2003.
- C9 P. Kitsos, S. Goudevenos and O. Koufopavlou, "VLSI Implementations of the Triple-DES Block Cipher", In proc. of *10th IEEE International Conference on Electronics, Circuits and Systems (ICECS'03)*, United Arab Emirates, December 14-17, 2003.
- C8 P. Kitsos, G. Theodoridis, and O. Koufopavlou, "An Reconfigurable Multiplier in  $GF(2^m)$  for Elliptic Curve Cryptosystem", In proc. of *10th IEEE International Conference on Electronics, Circuits and Systems (ICECS'03)*, United Arab Emirates, December 14-17, 2003.
- C7 N. Sklavos, P. Kitsos and O. Koufopavlou, "VLSI Implementation of Password (PIN) Authentication Unit", In proc. of *IEEE International Conference on Electronics, Circuits and Systems (ICECS'02)*, Croatia, September 15-18, 2002.
- C6 P. Kitsos, N. Sklavos and O. Koufopavlou, "An Efficient Implementation of the Digital Signature Algorithm", In proc. of *IEEE International Conference on Electronics, Circuits and Systems (ICECS'02)*, Croatia, September 15-18, 2002.
- C5 N. Sklavos, K. Papadomanolakis, P. Kitsos and O. Koufopavlou, "Euclidean Algorithm VLSI Implementations", In proc. of *IEEE International Conference on Electronics, Circuits and Systems (ICECS'02)*, Croatia, September 15-18, 2002.
- C4 P. Kitsos, N. Sklavos and O. Koufopavlou, "Hardware Implementation of the SAFER+ Encryption Algorithm for the Bluetooth System", In proc. of *IEEE International Symposium on Circuits & Systems (ISCAS'02)*, USA, May 26-29, 2002.
- C3 N. Sklavos, P. Kitsos, K. Papadomanolakis and O. Koufopavlou, "Random Number Generator Architecture and VLSI Implementation", In proc. of *IEEE International Symposium on Circuits & Systems (ISCAS'02)*, USA, May 26-29, 2002.
- C2 P. Kitsos, N. Sklavos, N. Zervas and O. Koufopavlou, "A Reconfigurable Linear Feedback Shift Register (LFSR) for the Bluetooth System", In proc. of *IEEE International Conference on Electronics, Circuits and Systems (ICECS'01)*, Malta, September 2-5, 2001.
- C1 N. Sklavos, P. Kitsos, N. Zervas and O. Koufopavlou, "A New Low Power and High Speed Bidirectional Shift Register Architecture", In proc. of *International Workshop on Power And Timing Modelling, Optimization and Simulation (PATMOS'01)*, Switzerland, September 26-28, 2001.

## **V. Tutorials in conference proceedings**

- T6 O. Koufopavlou, G. Selimis, N. Sklavos, and P. Kitsos, "Cryptography: Circuits and Systems Approach", *5<sup>th</sup> IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'05)*, Greece, December 18-21, 2005.

- T5 O. Koufopavlou, G. Selimis, N. Sklavos, P. Kitsos, "Cryptography: Circuits and Systems Approach", In *proc. of International Workshop on Power And Timing Modelling, Optimization and Simulation (PATMOS'05)*, Leuven, Belgium, September 20-23, 2005.
- T4 P. Kitsos, O. Koufopavlou, G. Selimis, and N. Sklavos, "Low Power Cryptography", *Second Conference Conference On Microelectronics, Microsystems and NanoTechnology, (MMN'04)*, Greece, November 14-17, 2004.
- T3 O. Koufopavlou, N. Sklavos and P. Kitsos, "Cryptography: Circuits and Systems Approach", *4<sup>th</sup> Marlow Workshop*, September 14<sup>th</sup> 2004, Isle of Santorini, Greece.
- T2 P. Kitsos, O. Koufopavlou, and N. Sklavos, "Cryptography: Circuits and Systems Approach", *IEEE International Symposium on Circuits & Systems (ISCAS'04)*, Canada, May 23-26, 2004.
- T1 O. Koufopavlou, N. Sklavos and P. Kitsos, "Cryptography in Wireless Protocols: Hardware and Software Implementations", *IEEE International Symposium on Circuits and Systems (ISCAS'03)*, Thailand, May 25-28, 2003.

## **V. Others Publications**

- O4. Shiguo Lian, Yan Zhang, Jong Hyuk Park, Paris Kitsos, "Guest Editors' Introduction to the Special Issue on Secure Multimedia Communication", *Security and Communication Networks* (Wiley), Volume 1, Issue 6, pages 437–440, November/December 2008.
- O3. P. Kitsos and N. Sklavos, "Guest Editors' Introduction to the Special Issue on Security of Computers and Networks", *Computers and Electrical Engineering Journal (Elsevier Ltd.)*, Volume 33, Issue 5-6, Pages 321-323, September, 2007.
- O2 P. Kitsos, "System-on-Chip Architectures and Implementations for Private-Key Data Encryption-A Review", *IEEE Circuits and Devices Magazine*, Volume 21, Issue 6, Jan.-Feb. 2006 Page(s): 54 – 56.
- O1 Paris Kitsos, "On the hardware implementation of the Mickey-128 stream cipher", *Cryptology ePrint Archive*, Report 2005/301, 2005. Also in eSTREAM, <http://www.ecrypt.eu.org/stream/papersdir/2006/059.pdf>

## **13. INVITED LECTURES**

- 03/07/2012 "Block Ciphers in FPGA Design: A Case Study of SEED Block Cipher", 3rd IEEE Greece GOLD A.G. ATHENA Summer School, Pyrgos, GREECE, 1 to 6 July, 2012.
- 24/05/2011 "FPGA-based Considerations of SEED Block Cipher", The Claude Shannon Institute Workshop for Coding and Cryptography - CSI-WCC 2011, University of College Cork, Cork, Ireland.
- 29/03/2007 "Hardware Architectures of the Whirlpool Hash Function", Information and Communication Systems Engineering Department, University of the Aegean, Greece.
- 16/02/2007 "Applied Cryptography and Hardware Architectures", Cyprus University of Technology, Lemesos, Cyprus.

## **14. ACADEMIC SERVICES**

- Served as a *reviewer* for *international journals*  
-IEEE Transactions on Computers.

- IEEE Transactions on Very Large Scale Integration.
  - IEEE Transactions on Circuits and Systems-I (TCAS-I).
  - IEEE Transactions on Circuits and Systems-II (TCAS-II).
  - IEEE Transactions on Parallel and Distributed Systems.
  - IEEE Proceedings Journal.
  - IEEE Computer Magazine.
  - IEEE Multimedia Magazine.
  - IEEE-Proceedings on Computers and Digital Techniques, Journal.
  - IEEE Proceedings on Information Security, Journal.
  - ACM Transactions on Embedded Computing Systems Journal.
  - Elsevier Journal of Computational and Applied Mathematics.
  - Integration, the VLSI Journal, Elsevier Ltd.
  - Elsevier Microelectronics Journal, Circuits and Systems.
  - Elsevier Journal of Systems Architecture.
  - Computers and Electrical Engineering Journal, Elsevier Ltd.
  - Journal of Supercomputing, Springer.
  - Wireless Personal Communications, Springer.
  - Journal of Real-Time Image Processing, Springer.
  - The Computer Journal, OXFORD University Press.
- Served as a *reviewer* for *international conferences*
    - IEEE, International Conferences on Electronics, Circuits and Systems (ICECS).
    - IEEE, International Symposium on Circuits and Systems (ISCAS).
    - IEEE, Midwest Symposium on Circuits and Systems (MWSCAS).
    - IEEE, Mediterranean Electrotechnical Conference (MELECON).
    - IEEE International Conference on Communications (ICC), Signal Processing for Communications.
    - IEEE International Conference on Telecommunications (ConTEL).
    - IEEE The International Conference on “Computer as a Tool” (EUROCON).
    - IEEE Workshop on Signal Processing Systems (SIPS).
    - European Conference on Circuit Theory and Design (ECCTD).
    - World Automation Congress (WAC).
    - International Conference on Communication Systems, Networks and Digital Signal Processing (CSNDSP).
    - International Conference on Computer, Communication and Control Technologies (CCCT).
    - International conference on High Performance Computing and Communications. Special Session: Pervasive Computing Application & Security Service (PCASS).
    - The Second IEEE International Symposium on Pervasive Computing and Ad Hoc Communications (PCAC).
    - International Conference on Intelligent Computing (ICIC).
    - IEEE International Conference on Industrial Technology (ICIT)

## **15 JOURNALS & CONFERENCE PARTICIPATION IN ORGANIZATION**

### **I) Committee Member and Guest Editor for Journals**

- *Guest co-editor of the Special Issue on “Smart Grid Communications Systems”, IEEE Systems Journal (ISJ), 2012.*
- *Guest co-editor of the Special Issue on “Digital System Security and Safety”, Microprocessors and Microsystems: Embedded Hardware Design (MICPRO) (Elsevier Ltd.), 2012.*

- *Associate Editor of IEEE Systems Journal*. From January 2011 to today.
- *Associate Editor of Microprocessors and Microsystems: Embedded Hardware Design (MICPRO) (Elsevier Ltd.)*. From September 2010 to today.
- *Guest co-editor of the Special Issue on “Information Security and data protection in Future Generation Communication and Networking”, Wireless Personal Communications, An International Journal (Springer), 2009.*
- *Guest co-editor of the Special Issue on “Secure Multimedia Communication”, Wiley Journal: Security and Communication Network (SCN), Volume 1 Issue 6 (November/December 2008).*
- *Associate Editor of International Journal of Reconfigurable Computing (Hindawi Journal)*. From May 2007 to today.
- *Guest co-editor of the Special Issue on “Security of Computers & Networks”, Computer and Electrical Engineering, An International Journal (Elsevier Ltd.), Vol. 33, Issues 5-6, 2007.*
- *Editorial Board Member of Committee Member of “Computer and Electrical Engineering, An International Journal (Elsevier Ltd.)”*. From January 2006 to March 2011.

## **II) Organization Committee Member and Guest Editor for Conferences/Workshops**

- *Program Committee Member for “The 9th International Conference on ReConFigurable Computing and FPGA’s, (ReConFig’13)”, Dec 9, 2013 - Dec 11, 2013, Cancun, Mexico.*
- *Program Committee Member for “21st European Conference on Circuit Theory and Design (ECCTD 2013)”, 8 – 12 September 2013, Dresden, Germany.*
- *Special Session Organizer on “Architectures and Hardware for Security Applications”, 16th EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, Architectures, Methods and Tools - DSD’2013”, Santander, Spain, September 4-6, 2013.*
- *Program Committee Member for 16th Euromicro Conference on Digital System Design, Architectures, Methods and Tools – DSD 2013, Santander, Spain, September 4-6, 2013.*
- *Exhibits Chair for “18th International Conference on Digital Signal Processing”, 1-3 July 2013, Santorini, Greece.*
- *Program Committee Member for “ENGINEERING OF RECONFIGURABLE SYSTEMS AND ALGORITHMS - ERSA’13”, July 22-25, Las Vegas, Nevada, USA.*
- *Program Committee Member for “EUROMICRO/IEEE Workshop on Embedded and Cyber-Physical Systems (ECYPS’2013)”, Montenegro, Budva, June 19, 2013.*
- *Program Committee Member for “First Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE 2013)”, Avignon – France, May 30th-31st, 2013.*
- *Program Committee Member for “16th IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)”, Karlovy Vary, Czech Republic, April 8-10, 2013.*
- *Program Committee Member for “The 7th International Conference on ReConFigurable Computing and FPGA’s, (ReConFig’12)”, December 5-7, 2012, Cancun, Mexico.*

- *Program Committee Member for “ENGINEERING OF RECONFIGURABLE SYSTEMS AND ALGORITHMS - ERSA'12”*, July 16-19, 2012, Las Vegas, Nevada, USA.
- *Program Committee Member for “International Symposium on Electronic System Design (ISED) 2012”*, 21-23 December 2012, Kolkata, India.
- *Program Committee Member for 15th Euromicro Conference on Digital System Design, Architectures, Methods and Tools – DSD 2012*, Izmir, Turkey, 3-5 September, 2012.
- *Program Committee Member in Special Session entitled “European Projects in Digital System Design - (EPDSD)”*, *15th Euromicro Conference on Digital System Design, Architectures, Methods and Tools – DSD 2012*, Izmir, Turkey, 3-5 September, 2012.
- *Special Session Organizer “Architectures and Hardware for Security Applications (AHSA)”*, *15th Euromicro Conference on Digital System Design, Architectures, Methods and Tools – DSD 2012*, Izmir, Turkey, 3-5 September, 2012.
- *Program Committee Member for “International Symposium on Electronic System Design (ISED) 2011”*, 19-21 December 2011, Kochi, India.
- *Program Committee Member for “The 7th International Conference on ReConFigurable Computing and FPGA’s, (ReConFig’11)”*, Nov 30, 2011 - Dec 2, 2011, Cancun, Mexico.
- *Program Committee Member for “Workshop on Cryptographic Hardware and Embedded Systems 2011 (CHES 2011)”*, Nara, Japan, September 28th – October 1st 2011.
- *Program Chairman for “14th EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, Architectures, Methods and Tools - DSD’2011”*, Oulu, Finland, August 31 - September 2, 2011.
- *Special Session Co-organizer of the Special Session on “Architectures and Hardware for Security Applications”*, *14th EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, Architectures, Methods and Tools - DSD’2011”*, Oulu, Finland, August 31 - September 2, 2011.
- *Program Committee Member for “Fourth International Conference on New Technologies, Mobility and Security (NTMS 2011)”*, February 7 - 10, 2011, Paris - France.
- *Program Committee Member for “International Symposium on Electronic System Design (ISED) 2010”*, 20-22 December 2010, Bhubaneswar, India.
- *Guest Co-editor of the Special Session on “Cryptographic Hardware & Embedded Systems”*, *17th IEEE International Conference on Electronics, Circuits, and Systems (ICECS 2010)*, Athens, December 12-15, 2010.
- *Program Committee Member for “The 6th International Conference on ReConFigurable Computing and FPGA’s, ReConFig’10”*, December 6-8 2010, Cancun, Mexico.
- *Program Committee Member for “The 2nd International Workshop on Security in Cloud Computing (SCC’2010)”*, September 13-15 2010, San Diego, California, USA.
- *Deputy Program Chair for “13th EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, Architectures, Methods and Tools - DSD’2010”*, Lille, France, September 1-3, 2010.

- *Program Committee Member for “ENGINEERING OF RECONFIGURABLE SYSTEMS AND ALGORITHMS - ERSA'10”*, July 12-15, Las Vegas, Nevada, USA.
- *Program Committee Member for “2010 International Conference on High Performance Computing Systems (HPCS-10)”*, July 12-14 2010, Orlando, FL, USA.
- *Program Committee Member for “IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2010)”*, July 5-7 2010, Kefalonia, Greece.
- *Program Committee Member for “2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS2010)”*, June 25-27, 2010 in Beijing, China.
- *Program Committee Member for “2nd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems-MOBISEC 2010”*, May 26-28 2010, Catania, Sicily, Italy.
- *Program Committee Member for “The 5th International Conference on Future Information Technology (FutureTech 2010)”*, May 21-23, 2010, Busan, Korea.
- *Program Committee Member for “Design, Analysis and Tools for Integrated Circuits and Systems - IMECS 2010-DATICS-IMECS'10”*, Hong Kong, 17-19 March, 2010.
- *Program Committee Member for “The 5th International Conference on ReConFigurable Computing and FPGA's, ReConFig'09”*, December 9-11, 2009, Cancun, Mexico.
- *General Local Chair for “12th EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, Architectures, Methods and Tools - DSD'2009”*, Patras-Greece, August 27-29, 2009.
- *Program Committee Member for “2009 International Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-09)”*, July 13-16 2009, Orlando, FL, USA.
- *Program Committee Member for “ENGINEERING OF RECONFIGURABLE SYSTEMS AND ALGORITHMS - ERSA'09”*, July 13-16, Las Vegas, Nevada, USA, track of the conference “The 2009 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'09)”.
- *Program Committee Member for “16th International Conference on Digital Signal Processing (DSP 2009)”*, July 5-7 2009, Santorin Isle, Greece.
- *Program Committee Member for “IEEE DATICS-ICIEA'09, Design, Analysis and Tools for Integrated Circuits and Systems”*, Xian, China, May 25-27, 2009.
- *Program Committee Member for “DATICS-IMECS'09, Design, Analysis and Tools for Integrated Circuits and Systems”*, Hong Kong, March 18-20, 2009.
- *Program Committee Member and Track Co-chair for “The 4th International Conference on ReConFigurable Computing and FPGA's, ReConFig'08”*, December 3-5, 2008, Cancun, Mexico.



- *Program Committee Member and Session Chair for “11th EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, Architectures, Methods and Tools - DSD’2008”*, Parma, Italy, September, 3 - 5 Σεπτεμβρίου, 2008.
- *Program Committee Member for “ENGINEERING OF RECONFIGURABLE SYSTEMS AND ALGORITHMS - ERSA’08”*, July 14-17, Las Vegas, Nevada, USA, track of the conference “*The 2008 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP’08)*”.
- *Program Committee Member for “2008 International Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-08)”*, July 7-10 2008, Orlando, FL, USA.
- *Program Committee Member for “International Conference on Theoretical and Mathematical Foundations of Computer Science (TMFCS-08)”*, July 7-10, 2008, Orlando, FL, USA.
- *Program Committee Member for “The 5th International Conference on Ubiquitous Intelligence and Computing (UIC-08)”*, Organized by Oslo University College, Norway, June 23-25, 2008.
- *Program Committee Member for “IWRT 2008 - the 2nd International Workshop on RFID Technology - Concepts, Applications, Challenges”*, Barcelona, Spain, from 12 to 13 June 2008.
- *Program Committee Member for “Workshop on Security of Communication Systems (SCS-2008)”*, Damascus, Syria, April 9th, 2008.
- *Program Committee Member for “The 2nd International Workshop on Web and Pervasive Security (WPS2008)”*, Hong Kong, 17 - 21 March 2008.
- *Program Committee Member for “The 9th International Conference on Information and Communications Security (ICICS 2007)”*, Zhengzhou, Henan Province, China, 12-15 December, 2007.
- *Program Committee Member for “The 2nd International Workshop on Trustworthiness, Reliability and services in Ubiquitous and Sensor neTworks (TRUST 2007)”*, Taipei, Taiwan, December 10-13, 2007.
- *Program Committee Member for “Multimedia Networking and QoS Track”*, in conjunction with the “*IEEE International Symposium on Multimedia 2007*”, Taichung, Taiwan, December 10-12, 2007.
- *Publicity Co-Chair “The 2007 International Conference on Future Generation Communication and Networking (FGCN 2007)”*, December 6th ~ 8th, 2007, in Jeju Island, Korea.
- *Program Committee Member for “The 2nd International Symposium on Information Security (IS’07)”*, Iberian peninsula and islands, Oct 28 - Nov 2, 2007.
- *Program Committee Member for “The IEEE International Symposium on Integrated Circuits, ISIC-2007”*, Orchard Hotel, Signapore, 26 - 28 September 2007.
- *Program Committee Member for “3rd International Conference on Intelligent Environments (IE’07)”*, University of Ulm, Southern Germany, September 24 - 25, 2007.
- *Program Committee Member for “The IEEE Region 8 EUROCON 2007, International Conference on “Computer as a Tool”*, Warsaw, Poland, September 9-12, 2007.

- *Program Committee Member* for “*10th EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, Architectures, Methods and Tools - DSD’2007*”, Lübeck, Germany, August 29th - 31st, 2007.
- *Program Committee Member* for “*International Conference on Security and Cryptography, SECRYPT 2007*”, Barcelona – Spain, 28-31 July 2007.
- *Program Committee Member* for “*International Conference on Signal Processing and Multimedia Applications, SIGMAP 2007*”, Barcelona – Spain, 28-31 July 2007.
- *Program Committee Member* for “*2007 International Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-07)*”, 9-12 of July 2007, Orlando, FL, USA.
- *Program Committee Member* for “*ENGINEERING OF RECONFIGURABLE SYSTEMS AND ALGORITHMS - ERSA’07*”, June 25-28, Monte Carlo Resort, Las Vegas, Nevada, USA, a part of “*The 2007 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP’07)*”.
- *Program Committee Member* for “*The 2007 international Workshop on Application and Security Service in Web and pervasive eNvirionments (ASWAN ’07)*”, June 16-18, 2007, HuangShan (Yellow Mountains), China.
- *Program Committee Member* for “*The 4th International Workshop on Ubiquitous Computing (IWUC 2007)*” in conjunction with the “*9th International Conference on Enterprise Information Systems (ICEIS 2007)*”, 12-13 June, 2007 - Funchal, Madeira – Portugal.
- *Program Committee Member* for “*The 1st International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2007)*”, in conjunction with the “*9th International Conference on Enterprise Information Systems (ICEIS 2007)*”, 12 June, 2007 - Funchal, Madeira – Portugal.
- *Program Committee Member* for “*2007 International Conference on Multimedia and Ubiquitous Engineering (MUE 2007)*”, Seoul, Korea, April 26<sup>th</sup> ~ 28<sup>th</sup>, 2007.
- *Program Committee Member* for “*Eighth International Conference on Information and Communications Security (ICICS ’06)*”, Raleigh, North Carolina, USA, December 4-7, 2006.
- *Program Committee Member* for “*2006 International Conference on Hybrid Information Technology*”, International Convention Center, Cheju Island, Korea, November 9th ~ 11th, 2006.
- *Program Committee Member* for “*The 3rd International Conference on ReConFigurable Computing and FPGA’s, ReConFig’06*”, San Luis Potosi, Mexico, September 20-22, 2006.
- *Program Committee Member* for “*The 2006 International Conference on High Performance Computing and Communications*”, Munich, Germany, September 13-15, 2006.
- *Program Committee Member* for “*International Conference on Security and Cryptography, SECRYPT 2006*”, Setibal – Portugal, 7-10 August 2006.
- *Program Committee Member* for “*International Conference on Signal Processing and Multimedia Applications, SIGMAP 2006*”, Setibal – Portugal, 7-10 August 2006.

- *Technical Committee Member* for “*International Forum on Multimedia and Image Processing, IFMIP – World Automation Congress*”, WAC 2006, July 25-28, 2006.
- *Guest Co-editor* of the Special Session on “*Information Security and Hardware Implementations*”, International Forum on Multimedia and Image Processing, IFMIP – World Automation Congress, WAC 2006, July 25-28, 2006.
- *Technical Committee member* for “*2<sup>nd</sup> IEE International Conference on Intelligent Environments, IE’06*”, July 5-6, 2006, National University of Athens, Greece.
- *Technical Committee member* for “*The 2006 International Conference on Scientific Computing (CSC’06)*”, June 26-29, 2006, Las Vegas, USA.
- *Technical Committee member* for “*The 2006 International Conference on Security and Management (SAM’06)*”, June 26-29, 2006, Las Vegas, USA.
- *Technical Committee member* for “*The 2006 International Conference on Computer Design (CDES’06)*”, June 26-29, 2006, Las Vegas, USA.
- *Technical Committee member* for “*The 2006 International Conference on Embedded Systems and Applications (ESA’06)*”, June 26-29, 2006, Las Vegas, USA.
- *Guest Co-editor* of the Special Session on “*New Generation Architectures/Implementations for Security Protocols and Cryptography Applications*” IEEE International Symposium on Circuits and Systems (ISCAS 2006), Kos, Greece, May 21 - 24 2006.
- *Technical Program Committee* for “*IEEE Workshop on Signal Processing Systems (SIPS)– Design and Implementations*”, November 2-4, 2005, Athens, Greece.
- *Session chair* (in Information Processing session) of the “*International Arab Conference on Information Technology (ACIT 2001)*”, Jordan University of Science and Technology, Jordan, November 13th - 15th, 2001.

### **III) National Organizations**

Co-editor of the three monthly published newsletter “The Circuit” of the IEEE joint Greek Circuits and Systems and Solid-State Circuits chapters. From 01/11/2006 to 31/12/2009.

### **15. RECOGNITION**

- Received more than *500 non-self citations* on his research publications (Google Scholar Citations).
- Scholarship for his post-doc research from the Greek State Scholarships Foundation (2008-2009).