CURRICULUM VITAE
Dr. PARASKEVAS (PARIS) KITSOS

March 2023

1. PERSONAL DATA

Name:	Paraskevas (Paris) Kitsos
Birthday:	12 February 1975
Occupation:	Associate Professor
Nationality:	Greek
Marital status:	Married with two kids
Office address:	Electrical and Computer Engineering Department (ECE), University of the Peloponnese, Greece
Office phone:	+30 2610369216
E-mail:	kitsos@uop.gr

2. 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.

3. POSITIONS HELD

- Associate Professor in Electrical and Computer Engineering Department (ECE), University of Peloponnese, Greece. From 5/2019 – today.
- Head of "Technologies and Services of Smart Informatics and Communication Systems", Postgraduate Program in Electrical and Computer Engineering Department (ECE), University of Peloponnese, Greece. From 10/2021 – today.
- Assistant Professor in Computer & Informatics Engineering Department (CIED), Technological Educational Institute of Western Greece, Greece. From 5/2014 – 4/2019.
- Collaborating Faculty in Industrial System Institute (ISI), "Athena" Research Center, Patras, Greece. From 5/2014 – today.
- Research fellow in Industrial System Institute (ISI), "Athena" Research Center, Patras, Greece. From 1/2012 – 5/2014.
- Research fellow in Digital Systems & Media Computing Laboratory, School of Science & Technology, Hellenic Open University (HOU), Patras, Greece. From 6/2005 to 5/2015.

4. RESEARCH INTERESTS

- Hardware Trojans Detection Techniques
- Hardware architectures and implementations of cryptographic algorithms.
- Hardware Acceleration of ML
- Efficient architectures and implementations for DSP primitives.
- FPGA and ASIC design.
- Security for Industrial Systems.
- Hardware on IoT.
- VLSI design.

5. TEACHING EXPERIENCE

2019-2023

- Associate Professor with Electrical and Computer Engineering Department (ECE), University of the Peloponnese: Tutorships: "Secure Hardware Design", "FPGA-based Systems Design" and "Hardware Description Languages" and "Advanced Security Systems (Postgraduate)".

2018-2019

- Associate Professor with Computer & Informatics Engineering Department (CIED), Technological Educational Institute of Western: Tutorships: "Secure Hardware Design", "FPGA-based Systems Design" and "Hardware Description Languages" and "Advanced Security Systems (Postgraduate)".

2014-2018

- Assistant Professor with Computer & Informatics Engineering Department (CIED), Technological Educational Institute of Western: Tutorships: "Network Security", "Secure Hardware Design", "FPGA-based Systems Design" and "Hardware Description Languages" and DSP & Hardware (Postgraduate) and Principles of Security Systems (Postgraduate).

6. CONTRIBUTION TO RESEARCH PROJECTS

He has participated in many national and international research projects in his area as researcher, designer and programmer.

7. PUBLICATIONS

I. Books

7. N. Sklavos, P. Kitsos, A Practical Introduction to Hardware/Software Codesign, Greek Version, (Original Book, A Practical Introduction to Hardware/Software Codesign, Patrick R. Shaumont, 2nd Edition, Springer, 2013), New Tech Pub, ISBN:978-960-578-039-5, 2019.
6. Paris Kitsos, "Digital System Design: Architectures, Methods and Tools", Proceedings of 19th EUROMICRO Conference on Digital System Design (DSD), Limmasol, Cyprus, August 31st - September 2nd, 2016. Published by the IEEE Computer Society, ISBN-13: 978-1-5090-2816-0.
5. P. Kitsos, N. Sklavos, editors of, FPGA Based System Design , Greek Version, (Original Book, FPGA Based System Design, W. Wolf, Prentice Hall Publisher, 2004), New Tech Pub, ISBN: 978-960-6759-88-8, 2014.
4. Nicolas Sklavos, Michael Huebner, Diana Goehringer, Paris Kitsos, "System-Level Design Methodologies for Telecommunication", Springer-USA, 2013.
3. 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.
2. Y. Zhang and P. Kitsos (Editors), "Security in RFID and Sensor Networks", Auerbach Publications, ISBN-10: 1420068393, ISBN-13: 978-1420068399, 2009.
1. 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

8. Paris Kitsos, Nicolas Sklavos and Artemios G. Voyiatzis, "Ring Oscillators and Hardware Trojan Detection", Hardware Security and Trust: Design and Deployment of Integrated Circuits in a

Threatened Environment, Springer, 2017, ISBN: 978-3-319-44316-4.

7. Ricardo Chaves, Leonel Sousa, Nicolas Sklavos, Apostolos P. Fournaris, Georgina Kalogeridou, Paris Kitsos, Farhana Sheikh, "Secure Hashing: SHA-1, SHA-2, and SHA-3", Circuits and Systems for Security and Privacy, CRC Press, ISBN: 9781482236880, 2016.
6. 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.
5. 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.
4. 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.
3. 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.
2. 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.
1. 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

25. Stavros Kalapothas, Georgios Flamis, Paris Kitsos, "Efficient Edge-AI Application Deployment for FPGAs", *Information* – Open Access Journal, Vol. *13, No.* 6, 2022 279; (Included in ISI/SCI)
24. Ludwig Kapmel, Paris Kitsos, Dimitris Simos, "Locating Hardware Trojans Using Combinatorial Testing for Cryptographic Circuits", IEEE Access, Vol. 10, pp: 18787 - 18806, 2022, DOI: 10.1109/ACCESS.2022.3151378. (Included in ISI/SCI)
23. Konstantinos G. Liakos, Georgios K. Georgakilas, Fotis C. Plessas, Paris Kitsos, "GAINESIS: Generative Artificial Intelligence NEtlists SynthesIS", Electronics – Open Access Journal, Vol. 11, No. 2, 2022. (Included in ISI/SCI)
22. Georgios Flamis, Stavros Kalapothas, Paris Kitsos, "Best practices for the deployment of edge inference: The conclusions to start designing", Electronics – Open Access Journal, Vol. 10, 2021. (Included in ISI/SCI)
21. Kostas Efstathiou, Paris Kitsos, "Efficient Majority Logic Magnitude Comparator Design", Microprocessors and Microsystems: Embedded Hardware Design της Elsevier, Vol. 82, April 2021. (Included in ISI/SCI)
20. Lampros Pyrgas, Paris Kitsos, "Compact Hardware Architectures of Enocoro-128v2 Stream Cipher for Constrained Embedded Devices", Electronics – Open Access Journal, Vol. 9, Issue. 9, 1505-1519, 2020. (Included in ISI/SCI)
19. Filippos Pirpilidis, Lampros Pyrgas, Paris Kitsos, "An 8-bit Serialized Architecture of SEED Block Cipher for Constrained Devices", IET Circuits, Devices & Systems, Vol. 14, Issue 3, 2020. (Included in ISI/SCI)
18. Apostolos P. Fournaris, Lampros Pyrgas, Paris Kitsos, "An efficient multi-parameter approach for FPGA hardware Trojan detection", Microprocessors and Microsystems: Embedded Hardware Design της Elsevier, Vol. 71, November 2019. (Included in ISI/SCI)
17. Lampros Pyrgas, Paris Kitsos, Athanassios Skodras, "Compact FPGA Architectures for the Two-Band Fast Discrete Hartley Transform", Microprocessors and Microsystems: Embedded Hardware Design της Elsevier, Vol. 61, September 2018. (Included in ISI/SCI)

16. Filippos Pirpilidis, Kyriakos G. Stefanidis, Artemios G. Voyiatzis, and Paris Kitsos, "Effect analysis of ring oscillator length and hardware Trojan size on an FPGA-based Implementation of the AES algorithm", Microprocessors and Microsystems: Embedded Hardware Design της Elsevier, Vol: 54, October 2017. (Included in ISI/SCI)
15. Apostolos P. Fournaris, Ioannis Zafeirakis, Paris Kitsos and Odysseas Koufopavlou, "Comparing Elliptic Curve Point Multiplication Design Approaches for Cryptography" Microprocessors and Microsystems: Embedded Hardware Design της Elsevier, 2015. (Included in ISI/SCI)
14. E. Cuevas-Farfan, M. Morales-Sandoval, A. Morales-Reyes, C. Feregrino-Uribe, I. Algredo-Badilio, P. Kitsos, R. Cumplido, "Karatsuba-Ofman Multiplier with Integrated Modular Reduction for (2^m)", Advances in Electrical and Computer Engineering, Volume 13, Number 2, 2013. (Included in ISI/SCI)
13. 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 της Elsevier, Vol. 37, Issue 2, 2013. (Included in ISI/SCI)
12. Morales-Sandoval, C. Feregrino-Uribe, R. Cumplido, P. Kitsos, "Area/performance trade-off analysis of an FPGA digit-serial GF(2^m) Montgomery Multiplier based on LFSR", Computer and Electrical Engineering της Elsevier, Vol. 39, Issue 2, 2013. (Included in ISI/SCI)
11. 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)
10. M. Morales-Sandoval, C. Feregrino-Uribe, P. Kitsos, "Bit-Serial and Digit-Serial GF(2^m) Montgomery Multipliers using Linear Feedback Shift Registers", *IET Computers & Digital Techniques*, Vol. 5, Issue. 2, March 2011. (Included in ISI/SCI)
9. 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)
8. 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)
7. 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)
6. 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)
5. 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)
4. 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)
3. 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)

2. P. Kitsos, G. Theodoridis, and O. Koufopavlou, "An Efficient Reconfigurable Multiplier Architecture for Galois field GF(2^m)", *Elsevier Microelectronics Journal*, Vol. 34, Issue 10, October 2003, pp. 975-980. (Included in ISI/SCI)

1. 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

67. Georgios Flamis, Stavros Kalapothas and Paris Kitsos, "FPGA-SoC deployment of complex deep neural network for magnitude and phase computations in denoising of speech signal", 30th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI SOC 2022), October 3-5, Patras, Greece.
66. Georgios Flamis, Stavros Kalapothas and Paris Kitsos, "Workflow on CNN utilization and inference in FPGA for embedded applications", IEEE – 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM 2021), Preveza, Greece, September 24th-26th 2021.
65. L. Pyrgas, P. Kitsos, "5G Security: FPGA Implementation of SNOW-V Stream Cipher", 24th Euromicro Conference on Digital Systems (DSD'21), Palermo, Italy, September 1-3, 2021.
64. Stavros Kalapothas, Georgios Flamis and Paris Kitsos, "Importing Custom DNN Models on FPGAs", 9th International Conference on Cyber-Physical Systems and Internet-of-Things (CPS&IoT' 2021), Budva, Montenegro, June 7-10, 2021.
63. L. Pyrgas, A. Panagiotarou and P. Kitsos, "Are ring oscillators without a combinatorial loop good enough for Hardware Trojan detection?", 23rd Euromicro Conference on Digital Systems (DSD'20), Slovenia, August 26 – August 28, 2020.
62. L. Pyrgas, P. Kitsos, "An 8-Bit Compact Architecture of Lesamnta-LW Hash Function for Constrained Devices", 26th IEEE International Conference on Electronics Circuits and Systems (ICECS 2019), Genova, Italy, November 27 to 29, 2019.
61. K. Ampatzidis, D. Oikonomou, P. Kitsos, M. Rigou, "A Smart Home Energy Management System Based on Internet-of-Things", 5th Panhellenic Conference on Electronics and Telecommunications-PACET (2019), November 8-9, 2019, Volos, Greece.
60. L. Pyrgas, P. Kitsos, "A Very Compact Architecture of CLEFIA Block Cipher for Secure IoT Systems", 22nd Euromicro Conference on Digital Systems (DSD '19), Kallithea, Chalkidiki, Greece, August 28 - August 30, 2019.
59. A. Fanariotis, T. Orphanoudakis, V. Fotopoulos, P. Kitsos, "DSD-i1: A mixed functionality development board geared towards digital systems design education", 22nd Euromicro Conference on Digital Systems (DSD '19), Kallithea, Chalkidiki, Greece, August 28 - August 30, 2019.
58. Filippos Pirpilidis, Lampros Pyrgas, Paris Kitsos, "A 4-bit Architecture of SEED Block Cipher for IoT Applications", 25th IEEE International Conference on Electronics Circuits and Systems (ICECS 2018), Bordeaux, France, 9-12 December 2018.
57. Apostolos Fournaris, Lampros Pyrgas, Paris Kitsos, "An FPGA Hardware Trojan Detection Approach Based on Multiple Parameter Analysis", 21st Euromicro Conference on Digital Systems (DSD'18), Prague, Czech Republic, August 29 - August 31, 2018.
56. Lampros Pyrgas, Paris Kitsos, "A Hybrid FPGA Trojan Detection Technique Based-on Combinatorial Testing and On-chip Sensing", 14th International Symposium on Applied Reconfigurable Computing (ARC 2018), Santorini, Greece, May 2-4, 2018.
55. Lampros Pyrgas, Filippos Pirpilidis, Aliki Panayiotarou, Paris Kitsos, "Thermal Sensor Based Hardware Trojan Detection in FPGAs", 20th Euromicro Conference on Digital Systems Design (DSD 2017), Vienna, Austria, August 30-September 1, 2017.

54. Fotios Kounelis, Nicolas Sklavos, Paris Kitsos, "Run-Time Effect by Inserting Hardware Trojans, in Combinational Circuits", 20th Euromicro Conference on Digital Systems Design (DSD 2017), Vienna, Austria, August 30-September 1, 2017.
53. Lampros Pyrgas, Paris Kitsos and Athanassios N. Skodras, "An FPGA Design for the Two-Band Fast Discrete Hartley Transform", 16th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2016), Limassol, Cyprus, 12-14 December, 2016.
52. N. Sklavos, P. Kitsos, A. G. Voyiatzis, "On the Hardware Implementation Efficiency of CAESAR Authentication Ciphers for FPGA Devices", Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE'16), Barcelona, Spain, November 14-16, 2016.
51. Filippos Pirpilidis, Artemios G. Voyiatzis, Lampros Pyrgas, Paris Kitsos, "An Efficient Reconfigurable Ring Oscillator for Hardware Trojan Detection", 20th Pan-Hellenic Conference on Informatics (PCI 2016), Patras, Greece, November 10th-12th, 2016.
50. Paris Kitsos, Kyriakos G. Stefanidis, Artemios G. Voyiatzis, "TERO-based Detection of Hardware Trojans on FPGA Implementation of the AES Algorithm", 19th Euromicro Conference on Digital Systems Design (DSD 2016), Limassol, Cyprus, August 31-September 2, 2016.
49. Artemios G. Voyiatzis, Kyriakos G. Stefanidis, Paris Kitsos, "Efficient Triggering of Trojan Hardware Logic", 19th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2016), Kosice, Slovakia, April 20-22, 2016.
48. Paris Kitsos, Dimitris Simos, Kyriakos Stefanidis and Artemios G. Voyiatzis, "Malicious hardware logic detection based on combinatorial testing", Fourth Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (Trudevice 2016), co located with Design Automation and Test in Europe (DATE 2016), Dresden, Germany, 14-18 March, 2016.
47. Paris Kitsos, Dimitris. E. Simos, Jose Torres-Jimenez, Artemios G. Voyiatzis "Exciting FPGA Cryptographic Trojans using Combinatorial Testing", 26th IEEE International Symposium on Software Reliability Engineering (ISSRE 2015), Gaithersburg, MD, USA, November 2-5, 2015.
46. Paris Kitsos and Artemios G. Voyiatzis, "TERO vs. RO for Hardware Trojan Horse Detection", *18th Euromicro Conference on Digital Systems Design (DSD'15),* Madeira, Portugal, 26-28 August, 2015.
45. Filippos Pirpilidis, Paris Kitsos, Athanasios Kakarountas, "A Compact Design of SEED Block Cipher", *4th Mediterranean Conference on Embedded Computing (MECO 2015),* Budva, Montenegro, 14-18, June 2015.
44. Paris Kitsos and Artemios G. Voyiatzis, "Investigating TERO for Hardware Trojan Horse Detection", Third Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (Trudevice 2015), co located with Design Automation and Test in Europe (DATE 2015), Grenoble, France, 9-13 March, 2015.
43. Paris Kitsos and Artemios G. Voyiatzis, "FPGA Trojan Detection Using Length-optimized Ring Oscillators", *17th Euromicro Conference on Digital Systems Design (DSD'14),* Verona, Italy, 27-29 August, 2014.
42. Paris Kitsos and Artemios G. Voyiatzis, "Advances in Detection of Hardware Trojan Horses", *3rd Mediterranean Conference on Embedded Computing (MECO 2014),* Budva, Montenegro, 15-19, June 2014.
41. Epameinontas Hatzidimitriou, Athanasios Kakarountas, Paris Kitsos, "Cipher Text Stealing Integrated in Implementations of IEEE P1619 for Shared Storage Media", *6th International Symposium on Communications, Control, and Signal Processing (ISCCSP 2014),* Athens, Greece, May 21-23, 2014.
40. F. Pirpilidis, P. Kitsos, N. Sklavos, "An Efficient FPGA-Based Architecture of Skein for Simple Hashing and MAC Function", *16th Euromicro Conference on Digital Systems Design (DSD'13),* Santander, Cantabria, Spain, 4-6 September, 2013.

39. 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.
38. G. Provelengios, P. Kitsos, N. Sklavos, C. Koulamas, "FPGA-based Design Approaches of Keccak Hash Function", *15th Euromicro Conference on Digital Systems Design (DSD'12),* Izmir, Turkey, 5-8 September, 2012.
37. 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.
36. P. Kitsos, N. Sklavos and A. N. Skodras, "A FPGA Implementation of the ZUC Stream Cipher", *14th Euromicro Conference on Digital Systems Design (DSD'11),* Oulu, Finland, August 31 - September 2, 2011.
35. G. Provelengios, N. Voros and P. Kitsos, "Low Power FPGA Implementations of JH and Fugue Hash Functions", *14th Euromicro Conference on Digital Systems Design (DSD'11),* Oulu, Finland, August 31 - September 2, 2011.
34. 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.
33. 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.
32. Paris Kitsos, Nicolas Sklavos, Athanassios N. Skodras, "Low Power FPGA Implementations of 256-bit Luffa Hash Function", *13th Euromicro Conference on Digital Systems Design (DSD'10),* Lille, France, September 1-3, 2010.
31. 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.
30. 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.
29. 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 Design, Architectures, Methods and Tools, DSD 2008*, Parma Italy, 3 - 5 September, 2008.
28. 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.
27. 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.
26. 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.
25. J. Daemen and P. Kitsos, "The self-synchronizing stream cipher Moustique", *eSTREAM Phase 2, the ECRYPT Stream Cipher Project, (ECRYPT NoE*). August 2006.
24. 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.
23. 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.

22 J. Daemen and P. Kitsos, "The self-synchronizing stream cipher Mosquito", *First Phase of ECRYPT Stream Cipher* Project Report 2005/018, 2005, Scandinavian Congress Center, Aarhus, Denmark, 26-27 May 2005. Η εργασία αυτή έχει παρουσιαστεί επίσης και στο *Symmetric Key Encryption Workshop (SKEW)* κατά την διάρκεια της παρουσίασης του ECRYPT project, Scandinavian Congress Center, Aarhus, Denmark, 26-27 May 2005.

21 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.

20 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.

19 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.

18 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.

17 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 (προσκαλεσμένη εργασία).

16 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.

15 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.

14 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.

13 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.

12 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.

11 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.

10 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.

9 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.

8 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.

7 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.

6 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.

5 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.

4 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.

3 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.

2 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.

1 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 Modeling, 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", *5th 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", *4th Marlow Workshop*, September 14th 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.

8. 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.
17/09/2014	"Σχεδιασμός Υλικού Ενσωματωμένων Συστημάτων σε FPGAs", 1ο Θερινό Σχολείο ΣΔΥ-ΕΑΠ, Τεχνολογίες Ασύρματων και Κινητών Επικοινωνιών & Εφαρμογές Κινητού και Διάχυτου Υπολογισμού, 08 - 20 Σεπτεμβρίου 2014, Θεσσαλονίκη, Ελλάδα.
07/07/2017	"Hardware Trojan Detection Techniques", Design Test Verification and EDA (DTVEDA) Workshop, Volos, Greece, 6-7 July 2017.
28/08/2017	"Detection of Hardware Trojans - Lab tutorial", Norwegian Computer and Information Security (COINS) summer school 2017 on Secure Implementation of Cryptographic Software, Metochi on Lesvos island, Greece, 27 August – 3 September, 2017.
01/10/2017 - 30/09/2018	Visitor Professor at the University of Pavia, Dept. of Electrical, Computer and Biomedical Engineering, Industrial Informatics and Embedded Systems MSc Program, Computer Engineering course, 12 hours lectures about Cryptography, Secure Hardware and FPGA-based Design of Digital Systems.
31/05/2021-02/06/2021	Summer School "8th Regional Growth Conference" in the framework of Regional Growth Conference 2021, "Advance Security Systems".
06/06/2022-11/06/2022	Summer School 2022, "Intelligent Cities: Technologies and Services of Smart Information Systems" in the framework of Regional Growth Conference 2022, "Secure Chips: Hardware Trojan Example".

9. JOURNALS & CONFERENCE PARTICIPATION IN ORGANIZATION

He has been Guest Editor of Special Issues for IEEE, Elsevier, Springer and Wiley publishers. In addition, he has participated to the organization of up to 140 conferences as Local Chair, Publicity, Program Chair and Program Committee member. In addition, he is reviewer for numerous International Journals and Conferences/Workshops in the area of his research.