Michail Maniatakos CV (as of Jan'14)

Assistant Professor
Electrical and Computer Engineering
New York University Abu Dhabi
Abu Dhabi, UAE

Contact: New York University Abu Dhabi
P.O. Box 129188, Abu Dhabi, UAE
Office: +971 2 628 4591, Cell: +971 56 689 7585
E-mail: michail.maniatakos@nyu.edu

Research Interests

- Encrypted general-purpose computation
- Robust microprocessor architectures
- Heterogeneous computer architectures

Education

Yale University, Electrical Engineering Department 2007-2012
- **Ph.D.** in Electrical Engineering 2012
- **M.Phil.** in Electrical Engineering 2010
- **M.Sc.** in Electrical Engineering 2009

University of Piraeus, Department of Informatics 2002-2007
- **M.Sc.** in Computing Systems Technology (Honors, 1st in class) 2007
- **B.Sc.** in Informatics (Honors, 1st in class) 2006

Professional Positions

Current:

Assistant Professor, New York University Abu Dhabi, ECE Dept. 2012-
Research Assistant Professor, Polytechnic Institute of NYU, ECE Dept. 2013-
Affiliated Faculty, Center for Interdisciplinary Studies in Security and Privacy, New York University Abu Dhabi 2013-

Past:

Assistant Professor/Faculty Fellow, Polytechnic Institute of NYU 2012-2013
Visiting Graduate Scholar, University of Texas at Dallas, TRELA Lab 2011-2012
Graduate Technical Intern, Intel Corporation, Santa Clara, CA 2008, 2010
Research Assistant, Yale University, TRELA Lab 2007-2012

Sponsored Research

Current:

NYUAD Research Enhancement Fund, Amount: $99K (Single-PI),
Title: 'Workload and Behavior Cognizant Cross-Layer Methodology for Low-Power Microprocessor Architectures', 09/13-08/15

Consolidated Edison, Amount: $393K (PI. Co-PI: Ramesh Karri, NYU-Poly),
Title: 'Platform Profiling in Legacy and Modern Control and Monitoring Systems', 1/14-12/15

Honors

- 1st place in Embedded System Challenge competition, CSAW X 2013
- 1st place in Malicious Processor design competition, CSAW VIII 2011
- IEEE TTTC Gerald W. Gordon Award for exceptional community service 2011
- Yale Faculty of Engineering, Fellowship Award 2007-2008
- University of Piraeus, Graduate Scholarship Award 2006-2007
- Greek State Scholarship Foundation, Undergraduate Scholarship 2003-2006
- University of Piraeus Honors Graduate (1st in class) 2006

Course Instructor

Polytechnic Institute of New York University

- EL-9433: Special Topics on Modern Microprocessors — Spring '13

New York University Abu Dhabi

- ENGR-AD-202: Computer Systems Programming — Summer '13
- ENGR-AD-313: Embedded Systems — Spring '14

Current Ph.D. Advisees

- Nektarios Tsoutsos, 1st year PhD student
  (Tentative) Topic: 'Homomorphically encrypted one instruction computer'
- Charalambos Konstantinou, 1st year PhD student
  (Tentative) Topic: 'Platform profiling in legacy and modern control systems'

Ph.D. Committee Participation

- Arun Kanuparthi, PhD candidate, Polytechnic Institute of New York University
  Advisor: Ramesh Karri
- Jerry Becker, PhD candidate, Polytechnic Institute of New York University
  Advisor: Ramesh Karri

Guided Research Projects

Polytechnic Institute of New York University

- EL9953: Advanced Project I, Student: Dhaval Lalan
  Title: 'Exploring architectural adaptation for low-power processors' — Fall '13

New York University Abu Dhabi

- Research Assistanship, Student: Anastasis Keliris
  Title: 'Microarchitectural support for forensics' — Fall '13–

Institutional & Departmental Service

New York University Abu Dhabi

- Campus Life and Faculty Liaison Committee — 2013-
- Engineering Graduate Committee — 2013-
- NYUAD Annual Research Conference Engineering Program Committee — 2014

Peer-reviewed journal publications

[1] N.G. Tsoutsos and **M. Maniatakos**. "Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation". In: *Special Issue of IEEE Transactions on Emerging Topics in Computing on Emerging Nanoscale Architectures for Hardware Security, Trust, and Reliability* ((accepted))

[2] N. Karimi, **M. Maniatakos**, C. Tirumurti, and Y. Makris. "On the Impact of Performance Faults in Modern Microprocessors". In: *Journal of Electronic Testing* 29.3 (2013), pp. 1480–1485

[3] **M. Maniatakos**, Y. Makris, P. Kudva, and B. Fleischer. "Low-cost Concurrent Error Detection for Floating Point Unit (FPU) Controllers". In: *IEEE Transactions on Computers* 62.7 (2013), pp. 1376–1388

[4] **M. Maniatakos**, C. Tirumurti, R. Galivanche, and Y. Makris. "Global Signal Vulnerability (GSV) Analysis for Selective State Element Hardening in Modern Microprocessors". In: *IEEE Transactions on Computers* 61.10 (2012), pp. 1361–1370

[5] **M. Maniatakos**, N. Karimi, A. Jas, C. Tirumurti, and Y. Makris. "Instruction-Level Impact Analysis of Low-Level Faults in a Modern Microprocessor Controller". In: *Special issue of IEEE Transactions on Computers on Concurrent On-Line Testing and Error/Fault Resilience of Digital Systems* 60.9 (2011), pp. 1260–1273

[6] N. Karimi, **M. Maniatakos**, A. Jas, C. Tirumurti, and Y. Makris. "Workload-Cognizant Concurrent Error Detection in the Scheduler of a Modern Microprocessor". In: *Special issue of IEEE Transactions on Computers on Concurrent On-Line Testing and Error/Fault Resilience of Digital Systems* 60.9 (2011), pp. 1274–1287

[7] Gizopoulos D., M. Psarakis, M. Hatzimihail, **M. Maniatakos**, A. Paschalis, A. Raghunathan, and Ravi S. "Systematic Software-Based Self-Test for Pipelined Processors". In: *IEEE Transactions on VLSI Systems* 16.11 (2008), pp. 1441–1453

PEER-REVIEWED CONFERENCE PUBLICATIONS

[8] N.G. Tsoutsos, C. Konstantinou, and **M. Maniatakos**. "Advanced Techniques for Designing Stealthy Hardware Trojans". In: *ACM Design Automation Conference*. 2014 (submitted)

[9] N.G. Tsoutsos and **M. Maniatakos**. "HEROIC: Homomorphically EncRypted One Instruction Computer". In: *IEEE Design, Automation and Test in Europe*. 2014 (accepted for presentation)

[10] **M. Maniatakos**, M. Michael, and Y. Makris. "Investigating the limits of AVF analysis in the presence of multiple bit errors". In: *IEEE International Online Testing Symposium*. 2013, pp. 49–54

[11] **M. Maniatakos**. "Privilege escalation attack through address space identifier corruption in untrusted modern processors". In: *IEEE Design and Technology of Integrated Systems*. 2013, pp. 161–166

[12] **M. Maniatakos**, M. Michael, and Y. Makris. "AVF-driven Parity Optimization for MBU Protection of In-core Memory Arrays". In: *IEEE Design, Automation and Test in Europe*. 2013, pp. 1480–1485

[13] **M. Maniatakos**, M. Michael, and Y. Makris. "Vulnerability-Based Interleaving for Multi-Bit Upset (MBU) Protection in Modern Microprocessors". In: *IEEE International Test Conference*. 2012, pp. 1–8

[14] Y. Jin, **M. Maniatakos**, and Y. Makris. "Exposing vulnerabilities of untrusted computing platforms". In: *IEEE International Conference on Computer Design*. 2012, pp. 91–96

[15] **M. Maniatakos**, C. Tirumurti, A. Jas, and Y. Makris. "AVF Analysis Acceleration via Hierarchical Fault Pruning". In: *IEEE European Test Symposium*. 2011, pp. 87–92

[16] **M. Maniatakos**, Y. Makris, P. Kudva, and B. Fleischer. "Exponent Monitoring for Low-Cost Concurrent Error Detection in FPU Control Logic". In: *IEEE VLSI Test Symposium*. 2011, pp. 235–240

[17] **M. Maniatakos** and Y. Makris. "Workload-driven selective hardening of control state elements in modern microprocessors". In: *IEEE VLSI Test Symposium*. 2010, pp. 159–164

[18] **M. Maniatakos**, N. Karimi, C. Tirumurti, A. Jas, and Y. Makris. "Instruction-Level Impact Comparison of RT- vs. Gate-Level Faults in a Modern Microprocessor Controller". In: *IEEE VLSI Test Symposium*. 2009, pp. 9–14

[19] N. Karimi, **M. Maniatakos**, C. Tirumurti, A. Jas, and Y. Makris. "Impact Analysis of Performance Faults in Modern Microprocessors". In: *IEEE International Conference on Computer Design*. 2009, pp. 91–96

[20] **M. Maniatakos**, N. Karimi, Y. Makris, A. Jas, and C. Tirumurti. "Design and Evaluation of a Timestamp-Based Concurrent Error Detection Method (CED)

in a Modern Microprocessor Controller". In: *IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems*. 2008, pp. 454–462

[21] N. Karimi, **M. Maniatakos**, Y. Makris, and A. Jas. "On the correlation between Controller Faults and Instruction-Level Errors in Modern Microprocessors". In: *International Test Conference*. 2008, pp. 24.1.1–24.1.10

INVITED CONFERENCE PUBLICATIONS

[22] N.G. Tsoutsos and **M. Maniatakos**. "Investigating the Application of One Instruction Set Computing for Encrypted Data Computation". In: *International Conference on Security, Privacy, and Applied Cryptography Engineering*. 2013, pp. 21–37

PATENTS

[1] **M. Maniatakos**, N.G. Tsoutsos, "'Homomorphically Encrypted One Instruction Computation"', (Provisional) U.S. Patent 61/924596, 2014

INVITED PRESENTATIONS

Topic: 'Fault injection infrastructure for the Alpha 21264 processor'

- **Intel Corporation**, Santa Clara, CA — Jan '08

Topic: 'Concurrent error detection in modern microprocessors'

- **Intel Corporation**, Santa Clara, CA — May '09

Topic: 'Enhancing robustness in modern microprocessors'

- **Brown University**, Providence, RI — Feb '12
- **Polytechnic Institute of NYU**, New York, NY — Apr '12
- **University of Texas at Dallas**, Richardson, TX — Apr '12
- **New York University Abu Dhabi**, Abu Dhabi, UAE — May '12

Topic: 'Robust and secure microprocessors'

- **IBM T.J. Watson**, Yorktown Heights, NY — Jul '12

Topic: 'Privilege escalation attack through address space identifier corruption in untrusted modern processors'

- **IEEE VLSI Test Symposium (VTS)**, Berkeley, CA — Apr '13

Topic: 'Investigating the Application of OISC for Encrypted Computation'

- **IBM T.J. Watson**, Yorktown Heights, NY — Sep '13
- **IEEE International Test Conference (ITC)**, Anaheim, CA — Sep '13
- **Columbia University**, New York, NY — Sep '13
- **Army Research Office Workshop on Trustworthy Hardware**, New York, NY — Nov '13

Topic: 'Security Applications of One Instruction Set Computing (OISC) Architectures'

- **IEEE International Conference Security, Privacy, and Applied Cryptography Engineering (SPACE)**, IIT Kharagpur, India — Oct '13

Topic: 'Enhancing the cyber-security of microprocessor-based industrial control systems'

- **Petroleum Institute**, Abu Dhabi, UAE — Nov '13

Topic: 'Enabling Secure Computation on the Cloud'

- **Research Workshop on Emerging Data Center and Cloud Computing Technologies**, UAEU University, Abu Dhabi, UAE — Dec '13

Topic: 'Platform Profiling in Legacy Power Grid and Emerging Smart Grid Environment'

- **Consolidated Edison**, New York, NY Jan '14

Professional Service

Workshop Organizer:

- 2nd 'Do You Trust Your Chip?' Workshop: Protecting the new generation of processing architectures Apr '13

Panelist:

- National Science Foundation (NSF) May '13

Organizing Committee:

- IEEE Design and Technology of Integrated Systems (DTIS) Mar '13

Special Session Organizer:

- Special Session: E.J. McCluskey Doctoral Thesis Competition, IEEE VLSI Test Symposium (VTS) Apr '13, Apr '14
- Crowd-sourcing hardware security research with a red team/blue team challenge process, Design and Automation Conference (DAC), Jun '14

Session Chair/Moderator:

- IEEE International Conference on Computer Design (ICCD) Sep '12
- IEEE VLSI Test Symposium (VTS) Apr '13, Apr '14
- International Conference on Security, Privacy and Cryptography Engineering (SPACE) Oct '13
- Army Research Office Workshop on Trustworthy Hardware, New York, NY Nov '13
- Design and Automation Conference (DAC) Jun '14
- NYU Abu Dhabi Research Conference Feb '14

Local Chair/Coordinator:

- IEEE International Symposium on Defect and Fault Tolerance in VLSI (DFT) Oct '13
- IEEE International Symposium on Nanoscale Architectures (NANOARCH) Jul '13

Technical Program Committee member:

- IEEE International Conference on Computer Design (ICCD) Sep '12, Oct '13
- IEEE International Symposium on Defect and Fault Tolerance in VLSI (DFT) Oct '12
- IEEE Design and Technology of Integrated Systems (DTIS) Mar '13, May '14
- IEEE International Test Conference (ITC), Sep '14
- IEEE International Symposium on VLSI (ISVLSI), Jul '14
- International Conference on Security, Privacy and Cryptography Engineering (SPACE) Oct '14

Technical referee:

- IEEE Transactions on Computers (T.COMP)
- IEEE Transactions on VLSI (T.VLSI)
- IEEE Transactions on Nanotechnology (T.NANO)
- IEEE Transactions on CAD (T.CAD)
- IEEE Transactions on Information Forensics and Security
- ACM Transactions on Embedded Computing Systems (TECS)
- ACM Journal of Emerging Technologies in Computing (JETC)

- IEEE Journal of Electronic Testing (JETTA)
- IEEE International Test Conference (ITC)
- IEEE Design and Automation Conference (DAC)
- IEEE Design Automation and Test in Europe (DATE)
- IEEE European Test Symposium (ETS)
- IEEE VLSI Test Symposium (VTS)
- IEEE International Symposium on Defect and Fault Tolerance in VLSI (DFT)
- IEEE International Conference on Computer-Aided Design (ICCAD)
- IEEE On-line Testing Symposium (IOLTS)
- IEEE International Conference of Computer-Aided Design (ICCD)
- IEEE Design and Technology of Integrated Systems (DTIS)