Michail Maniatakos C.V. (as of Dec '20)

Associate Professor
Electrical and Computer Engineering
New York University Abu Dhabi

Contact:
UAE: +971 2 628 4591, US: +1 646 920 3656
michail.maniatakos@nyu.edu, @realMoMAlab

Research Interests

- Privacy-preserving general-purpose computation
- Industrial control systems cybersecurity
- Additive manufacturing cybersecurity

Education

Yale University, Electrical Engineering Department '07–'12
- **Ph.D.** in Electrical Engineering '12
- **M.Phil.** in Electrical Engineering '10
- **M.Sc.** in Electrical Engineering '09

University of Piraeus, Department of Informatics '02–'07
- **M.Sc.** in Computing Systems Technology (Honors, 1st in class) '07
- **B.Sc.** in Informatics (Honors, 1st in class) '06

Professional Positions

Current:

Associate Professor, NYU Abu Dhabi, Engineering Division '19–
Global Network University Associate Professor, NYU Tandon School of Engineering, ECE '19–
Director of Education, NYU Abu Dhabi Center for Cyber Security '19–

Past:

Assistant Professor, NYU Abu Dhabi, Engineering Division '13–'19
Global Network University Assistant Professor, NYU Tandon School of Engineering, ECE '15–'19
Affiliated Faculty, Center for Cyber Security, NYU Abu Dhabi '13–'19
Research Assistant Professor, NYU Tandon School of Engineering, ECE '13–'16
Assistant Professor/Faculty Fellow, NYU Abu Dhabi, Engineering Div. '12–'13
Visiting Graduate Scholar, University of Texas at Dallas '11–'12
Graduate Technical Intern, Intel Corporation Summer '08, Summer '10
Research Assistant, Yale University '07–'11

Sponsored Research (Active)

Army Research Office (ARO), Amount: $17,666 (PI. Co-PI: Ramesh Karri), Title: 'Embedded security challenge: An education initiative focusing on cybersecurity' 06/20–06/21

NYU Abu Dhabi Research Institute, Amount: $8,660,000 (Co-PI. PI: Ozgur Sinanoglu), Title: 'Center for Cyber Security' 9/19–8/24

Abu Dhabi Department of Education and Knowledge, Amount: $184,834 (ADEK $81,688 cash support – NYUAD Institute $103,146 cost share), (PI. Co-PI: Ahmed Al Durra, Khalifa University), Title: 'Cyber-Security Testbed for Smart-City Power Grid' 1/19–12/20

Defense Advanced Research Projects Agency (DARPA), NYU share amount: $785,000 (Co-PI. PI: Ramesh Karri), Title: 'TIGR: Threat Intelligence for Grid Recovery' subcontract from SRI (total amount: $7M) 8/16–7/20

Past Sponsored Research

NYU Global Seed Grants, Amount: $130,906 (PI. Co-PI: Brendan Dolan-Gavitt), Title: 'Firmware emulation platform for smart-grid devices' 9/15–8/19

US Office of Naval Research (ONR), Amount: $35,610 (Single PI), Title: 'Covert data exfiltration from Internet-of-Things devices' 9/18–8/19

GlobalFoundries and NYUAD Institute, Amount: $2,570,702 (GlobalFoundries $1,396,604 in-kind support – NYUAD Institute match by $1,174,098 cash support), (co-PI. PI: Ozgur Sinanoglu) Title: 'TwinLab on Hardware Security and Trust', 6/15–5/19

US Office of Naval Research (ONR), Amount: $496,000 (PI. Co-PIs: Ramesh Karri, Farshad Khorrami), Title: 'Towards Automatic Vulnerability Assessment of Industrial Control Systems' 4/15–5/19

US Office of Naval Research (ONR), Amount: $35,292 (Single PI), Title: 'Programmable Logic Challenge: A Red team-Blue team stress test for state of the art PLC defense' 7/17–6/18

US Office of Naval Research (ONR), Amount: $142,000 (PI. Co-PIs: Ramesh Karri, Farshad Khorrami), Title: 'Instrumentation for Vulnerability Assessment of Industrial Control Systems' 9/16–4/18

Petroleum Institute, Amount: $115,000 (Petroleum Institute $55,000 cash support – NYUAD match by $60,000 support), (co-PI. PIs: Ahmed Al Durra, S.M. Muyeen), Title: 'Smart-grid extensions for Micro-grids – Stability, Security and privacy challenges' 9/15–8/16

Consolidated Edison, Inc., Amount: $393,000 (PI. Co-PI: Ramesh Karri), Title: 'Platform Profiling in Legacy and Modern Control and Monitoring Systems' 1/14–12/15

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

Honorable Mentions[1]:
National Science Foundation (NSF), Amount: $208,058 (Single PI), Title: 'TWC: Small: A hardware architecture for general-purpose computation using encrypted operands' 9/13–8/16

National Science Foundation (NSF), Amount: $499,918 (co-PI. PI: Ramesh Karri), Title: 'SaTC: STARSS: Hardware performance counters platform for enhancing security and privacy in high-performance and embedded processors' 9/13–8/16

[1]The proposals were returned after panel review and during the recommendation phase, because of a cost-sharing issue identified during budget check. NYU grants office's mistake prevented the grants to be funded.

Donations

Research Donations
Intel Corporation, Equipment Donation: Intel Xeon Phi 5110P + Server, Topic: 'Accelerating cryptographic primitives using many-core, wide-vector architectures'

Wind River, Software Donation: Simics Full System Simulator,
Topic: 'Hardware-based forensic analysis'

Teaching Donations

ARM, Equipment Donation: Freescale Freedom KL25Z boards (x10)
Course: Embedded Systems
Intel Corporation, Equipment Donation: Gallileo board (x20)
Course: Embedded Systems

Honors

- "ConFirm: Detecting Firmware Modifications in Embedded Systems using Hardware Performance Counters" has been selected as a **Top Picks in Hardware and Embedded Security** (most influential papers for 2012–2017) '20
- "ICSREF: A Framework for Automated Reverse Engineering of Industrial Control Systems Binaries:" **Distinguished paper finalist**, Network and Distributed System Security Symposium (NDSS) '19
- **Best paper award** for "Low-budget Energy Sector Cyberattacks via Open Source Exploitation," IFIP/IEEE International Conference on Very Large Scale Integration '18
- Arab-American Frontiers Symposium Fellowship 11/18
- Ph.D. Advisee honor: 2nd place in PhD Forum, IFIP/IEEE International Conference on Very Large Scale Integration (Advisee: Anastasis Keliris) '18
- Ph.D. Advisee honor: Pearl Brownstein Doctoral Research Award for doctoral research showing the greatest promise (Advisee: Nektarios Georgios Tsoutsos) '18
- IEEE Senior Member '17
- Stavros Niarchos Foundation, Greek Diaspora Fellowship Award Summer '17
- **Disclosed CVE-2017-7905 vulnerability, Severity: 9.8/10** 04/17
- Featured in magazine cover, Mechanical Engineering 139.3 03/17
- **Best paper award** for "Efficient parallelization of the Discrete Wavelet Transform algorithm using memory-oblivious optimizations," International Workshop on Power and Timing Modeling, Optimization and Simulation '15
- Ph.D. Advisee honor: Deborah Rosenthal, MD Award for best Qualifying Exam (Advisee: Nektarios Georgios Tsoutsos) '14
- Research Group honor: 1st place in Embedded Systems Challenge, CSAW X '13
- 1st place in Malicious Processor design competition, CSAW VIII '11
- IEEE TTTC Gerald W. Gordon Award for exceptional community service '11
- Yale Faculty of Engineering, Fellowship Award '07–'08
- University of Piraeus, Graduate Scholarship Award (1st in class) '06–'07
- University of Piraeus, Computer Science Honors Graduate (1st in class) '06
- Greek State Scholarship Foundation, Annual Undergraduate Scholarship (1st in class) '03–'06

Select Media Coverage

- Harvard Business Review, "3D Printing Gives Hackers Entirely New Ways to Wreak Havoc" 10/17
  URL: hbr.org/2017/10/3d-printing-gives-hackers-entirely-new-ways-to-wreak-havoc
- BBC, "Power firms alerted on hack attack scenarios" 07/17
  URL: www.bbc.com/news/technology-40766757
- Reuters, "GE fixing bug in software after warning about power grid hacks" 04/17
  URL: www.reuters.com/article/us-cyber-generalelectric-power-idUSKBN17S23Y

Course Instructor

New York University Abu Dhabi

- ENGR-UH-3510: Data Structures and Algorithms — Fall '19
- ENGR-UH-3511: Computer Organization and Architecture — Fall '17, Fall '18, Fall '19
- CDAD-UH 1037Q: Cyberwarfare — Spring '19
- ENGR-AD-201: Advanced Digital Logic — Spring '17
- ENGR-AD-113: Digital Logic — Spring '17
- ENGR-AD-313: Embedded Systems — Spring '14, Spring '15, Spring '16
- ENGR-AD-368: Selected Topics: Hardware Security and Trust — Fall '14
- ENGR-AD-202: Computer Systems Programming — Summer '13

New York University Tandon School of Engineering

- ECE-GY-9463: Security Architectures for Industrial Control Systems — Spring '21
- ECE-GY-6433: Advanced Hardware Design — Fall '20
- EL9433: Special Topics on Modern Microprocessors — Spring '13

Capstone Supervisor

New York University Abu Dhabi

- Daria Zahaleanu, Brandon Shaun Chin Loy — '19/'20
  Topic: 'Private reality framework'
- Pranav Mehta — '18/'19
  Topic: 'Cosmic Ray Detector-based Random Number Generator'
- Christos Zoukos, Yasmin Farhan — '17/'18
  Topic: 'A portable supercomputer'
- Pedro Pacareu, Pablo Zafiria — '16/'17
  Topic: 'Development of a Red-Team-In-a-Box hardware platform'
- Yilkal Derebe Abe — '15/'16
  Topic: 'FPGA-based network for fast microprocessor simulation'
- Farah Shammout — '15/'16
  Topic: 'Wearable device & data system to monitor and recognize health conditions of laborers'

Guided Project Courses

New York University Tandon School of Engineering

- EL9953: Advanced Project I, Student: Manjot Singh — Spring '16
  Topic: 'Flash Memory Reverse Engineering and Firmware Analysis'
- EL9953: Advanced Project I, Student: Vandita Sharma — Spring '15
  Topic: 'Industrial control systems security'
- EL9941: Advanced Project III, Student: Ankita Rajput — Fall '14
  Topic: 'Floating-point support for fully homomorphic encryption'
- EL9953: Advanced Project I, Student: Dhaval Lalan — Fall '13
  Topic: 'Exploring architectural adaptation for low-power processors'

Internship Supervisor

New York University Tandon School of Engineering

- CP-GY 9941: Internship for PhD I, Student: Esha Sarkar — Summer '20
  Company: Intel Corporation
- CP-GY 9941: Internship for PhD I, Student: Dimitrios Tychalas — Summer '18
  Company: Intel Corporation
- CP-GY 9941: Internship for PhD I, Student: Anastasis Keliris — Summer '17
  Company: Red Balloon Security
- CP-GY 9941: Internship for PhD I, Student: Charalambos Konstantinou — Summer '15
  Company: Consolidated Edison
- CP-GY 9941: Internship for PhD I, Student: Nektarios Tsoutsos — Summer '14
  Company: Intel Corporation

GRADUATED PH.D. ADVISEES

New York University Tandon School of Engineering

- Nektarios Georgios Tsoutsos (CSE) '13–'17
  Thesis title: 'Private and trustworthy computing using additive cryptographic primitives'
  - Placement: Assistant Professor at University of Delaware, Electrical and Computer Engineering Department
- Charalambos Konstantinou (ECE) '13–'18
  Thesis Title: 'Leveraging hardware features to enhance the cybersecurity of the smart grid'
  - Placement: Assistant Professor at Florida State University, Electrical and Computer Engineering Department
- Anastasis Keliris (ECE) '14–'19
  Thesis Title: 'Automated formulation of attack vectors for industrial control systems security assessment'
  - Placement: Red Ballon Security

CURRENT PH.D. ADVISEES

New York University Tandon School of Engineering

- Dimitrios Tychalas (ECE) '16–
  Topic (tentative): 'Embedded systems firmware emulation'
- Esha Sarkar (ECE) '16–
  Topic (tentative): 'Adversarial machine learning'
- Prashant Rajput (CSE) '18–
  Topic (tentative): 'Embedded systems security'
- Yue Wang (ECE, co-advised with Saif Jabari) '18–
  Topic (tentative): 'Transportation systems security'

M.SC. ADVISEES

University of Kaiserslautern

- Muhammad Ashif '17–'18
  Topic: 'Over-the-air secure firmware upgrade for legacy programmable logic controllers' (co-advised with Peter Liggesmeyer)

PH.D. COMMITTEE PARTICIPATION

New York University Tandon School of Engineering

- Satwik Patnaik — Advisor: Ozgur Sinanoglu
- Abrajit Sengupta — Advisor: Ozgur Sinanoglu
- Jun Zhang — Advisor: Siddharth Garg
- Maria Isabel Mera — Advisor: Siddharth Garg
- Mohammad Yasin — Advisor: Ozgur Sinanoglu
- Vinayaka Jyothi — Advisor: Ramesh Karri
- Chandra Kumar Holenarasipur Suresh — Advisor: Ozgur Sinanoglu
- Jerry Becker — Advisor: Ramesh Karri
- Arun Kanuparthi — Advisor: Ramesh Karri

M.SC. COMMITTEE PARTICIPATION

Petroleum Institute

- Ahmed Musleh — Advisors: Ahmed Al Durra, S.M. Muyeen

Guided Research Projects

New York University Abu Dhabi

- Post-graduate Summer Research Assistantship: Daria Zahaleanu — Summer '20
  Topic: 'Face Recognition with Client–Server Split Computation: Measuring Similarity from Embeddings'
- Undergraduate Research Internship: Fei Yuan Ko — Summer '20
  Topic: 'Entropy-based Static Malware Detection Approach for PLCs'
- Undergraduate Research Internship: Lachlan Pham — Summer '20
  Topic: 'Utilizing Strings Embedded in ELFs for Malware Detection in PLCs'
- Undergraduate Research Internship: Deebthik Ravi — Summer '20
  Topic: 'Code and data separation using semantic segmentation of binaries'
- Undergraduate Research Internship: Aizaz Ansari — Summer '20
  Topic: 'Machine learning for binary analysis'
- Undergraduate Research Internship: Gautham Dinesh — Summer '20
  Topic: 'Replicating state-of-the-art code and data separation solutions'
- Undergraduate Research Internship: Gopika Krishnan — Summer '20
  Topic: 'Implementation of backdoor attacks on facial recognition systems'
- Undergraduate Research Internship: Zayd Maradni — Summer '20
  Topic: 'BFV Homomorphic Multiplication: From Go to C++'
- Undergraduate Research Internship: Maya Fayed — Summer '20
  Topic: 'Test of FHE frameworks and improve E3 documentation'
- Undergraduate Research Internship: Reem Hazim — Summer '20
  Topic: 'Test of FHE frameworks and improve E3 documentation'
- Research Assistanship: Hadjer Benkraouda — '18–'20
  Topic: 'Unknown binary analysis classification using semantic segmentation'
- Research Assistanship: Homer Gamil — '19–
  Topic: '(Tentative) Privacy-preserving computation'
- Undergraduate Research Internship: Sanja Kastratovic — Summer '19
  Topic: 'Usability comparison of fully homomorphic encryption frameworks'
- Undergraduate Research Internship: Barkin Simsek — Summer '19
  Topic: 'Creating incentives towards crowdsourcing cryptanalysis of state-of-the-art academic cryptosystems'
- Undergraduate Research Internship: Yeojin Jung — Summer '19
  Topic: 'Improving the usability of the E3 framework'
- Undergraduate Research Internship: Julie Liu — Summer '19
  Topic: 'Machine learning backdoors using image filters'
- Undergraduate Research Internship: Estelle Ocran — Summer '19
  Topic: 'Machine learning backdoor detection and suppression'
- Undergraduate Research Internship: Nick Park — Summer '19
  Topic: 'Reverse engineering of industrial control systems binaries'
- Research Assistanship: Prashant Rajput — '18
  Topic: 'Process-aware attacks for thermal desalination plants'
- Research Associateship: Oleg Mazonka — '14–'15, '17–
  Topic: 'General-purpose encrypted computation'
- Post-doctoral Fellowship: Eduardo Chielle — '16–
  Topic: 'Compiler support for general-purpose encrypted computation'
- Research Assistanship: Anastasis Bikos — '16–'17
  Topic: 'Input/output support for keyless encrypted computation'
- Post-graduate Summer Research Assistantship: Yilkal Derek Abe — Summer '16
  Topic: 'Secure outsourcing'
- Undergraduate Research Internship: Homer Gamil — Summer '17
  Topic: '3D printing security'
- Research Assistanship: Raghad Baiad — '15–'16
  Topic: 'Privacy-preserving IP verification'

- Post-graduate Summer Research Assistant: Noha Alfergani — Summer '15
  Topic: 'Performance evaluation of privacy-preserving architectures'
- Research Assistanship: Chen Zhang — '14–'15
  Topic: 'Privacy-preserving 3rd party IP verification'
- Virtual Internship: Abhinay Kumar (IIT Kanpur), — Summer '17
  Topic: 'OpenPLC Ladder Logic Circuits on Raspberry Pi'
- Virtual Internship: Ritesh Kumar (IIT Kanpur), — Summer '18
  Topic: 'Proof-of-concept code for the Spectre vulnerability'

Patents

[P3] N.G. Tsoutsos, N. Gupta, and M. Maniatakos. *Systems and methods for malware detection in additive manufactured parts*. Provisional Patent application (62/639,548). 2018

[P2] M. Maniatakos, C. Konstantinou, and A. Keliris. *Systems and methods for privacy-preserving functional ip verification utilizing fully homomorphic encryption*. Patent Pending (App. 2016/0254912). Publication date Sep. 1, 2016

[P1] M. Maniatakos and N.G. Tsoutsos. *Homomorphically encrypted one instruction computation systems and methods*. US Patent 9,619,658. Issued Apr. 11, 2017

Book Chapters

[BC4] X. Liu, A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos. "Assessment of Low-budget Targeted Cyberattacks Against Power Systems". In: *VLSI-SoC: Design and Engineering of Electronics Systems Based on New Computing Paradigms*. Springer, 2019

[BC3] A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos. "Open Source Intelligence for Energy Sector Cyberattacks". In: *Critical Infrastructure Security and Resilience*. Springer, 2019, pp. 261–281

[BC2] N.G. Tsoutsos and M. Maniatakos. "Lightweight Fault Tolerance for Secure Aggregation of Homomorphic Data". In: *Security and Fault Tolerance in Internet of Things*. Springer, 2019, pp. 87–110

[BC1] C. Konstantinou and M. Maniatakos. "Security analysis of smart grid". In: *Communication, Control and Security Challenges for the Smart Grid* 2 (2017), p. 451

Editorials

[E3] M. Maniatakos and Y. Zhang. "CPSIOTSEC'20: 2020 Joint Workshop on CPS&IoT Security and Privacy". In: *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2020, 2135—2136

[E2] M. Maniatakos. "Guest Editor Introduction: Embedded Security Challenge". In: *IEEE Embedded Systems Letters* 10.3 (2018), pp. 81–82

[E1] M. Maniatakos, A.A. Cardenas, and R. Karri. "Guest Editors' Introduction: Cyber-Physical Systems Security and Privacy". In: *IEEE Design and Test* 34.4 (2017), pp. 5–6

Journal publications

[J26] E. Chielle, N. G. Tsoutsos, O. Mazonka, and M. Maniatakos. "Encrypt-Everything-Everywhere: ISA Extensions for Private Computation". In: *IEEE Transactions on Dependable and Secure Computing* (2020), (preprint)

[J25] D. Tychalas, A. Keliris, and M. Maniatakos. "Stealthy Information Leakage through Peripheral Exploitation in Modern Embedded Systems". In: *IEEE Transactions on Device and Materials Reliability* 20.2 (2020), pp. 308–318

[J24] O. Mazonka, E. Sarkar, E. Chielle, N.G. Tsoutsos, and M. Maniatakos. "Practical Data-in-use Protection using Binary Decision Diagrams". In: *IEEE Access* 8 (2020), pp. 23847–23862

[J23] E. Sarkar, Y. AlKindi, and M. Maniatakos. "Backdoor Suppression in Neural Networks using Input Fuzzing and Majority Voting". In: *IEEE Design & Test* 37.2 (2020), pp. 103–110

[J22] C. Konstantinou and M. Maniatakos. "A Data-Based Detection Method Against False Data Injection Attacks". In: *IEEE Design & Test* 37.5 (2020), pp. 67–74

[J21] C. Konstantinou and M. Maniatakos. "Hardware-layer intelligence collection for smart grid embedded systems". In: *Journal of Hardware and Systems Security* 3.2 (2019), pp. 132–146

[J20] F. Chen, Y. Luo, N.G. Tsoutsos, M. Maniatakos, K. Shahin, and N. Gupta. "Embedding tracking codes in additive manufactured parts for product authentication". In: *Advanced Engineering Materials* (2018), p. 1800495 (**featured in cover**)

[J19] N.G. Tsoutsos and M. Maniatakos. "Anatomy of Memory Corruption Attacks and Mitigations in Embedded Systems". In: *IEEE Embedded Systems Letters* 10.3 (2018), pp. 95–98

[J18] D. Mouris, N.G. Tsoutsos, and M. Maniatakos. "TERMinator Suite: Benchmarking Privacy-Preserving Architectures". In: *IEEE Computer Architecture Letters* 17.2 (2018), pp. 122–125

[J17] N.G. Tsoutsos and M. Maniatakos. "Efficient Detection for Malicious and Random Errors in Additive Encrypted Computation". In: *IEEE Transactions on Computers* 67.1 (2018), pp. 16–31

[J16] C. Konstantinou, M. Sazos, A.S. Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos. "GPS Spoofing Effect on Phase Angle Monitoring and Control in an RTDS-based Hardware-In-The-Loop Environment". In: *IET Cyber-Physical Systems: Theory & Applications* 2.4 (2017), pp. 180–187

[J15] J. Giraldo, E. Sarkar, A. Cardenas, M. Maniatakos, and M. Kantarcioglu. "Security and Privacy in Cyber-Physical Systems: A Survey of Surveys". In: *IEEE Design & Test* 34.4 (2017), pp. 7–17

[J14] O. Mazonka, N.G. Tsoutsos, and M. Maniatakos. "Cryptoleq: A Heterogeneous Abstract Machine for Encrypted and Unencrypted Computation". In: *IEEE Transactions on Information Forensics and Security* 11.9 (2016), pp. 2123–2138

[J13] S.E. Zeltmann, N. Gupta, N.G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri. "Manufacturing and security challenges in 3D printing". In: *Journal of Materials* 68.7 (2016), pp. 1872–1881 (**Most read in Springer Engineering Journals for 2016**)

[J12] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. Sadeghi, M. Maniatakos, and R. Karri. "The cybersecurity landscape in industrial control systems". In: *Proceedings of the IEEE* 104.5 (2016), pp. 1039–1057

[J11] X. Wang, C. Konstantinou, M. Maniatakos, R. Karri, S. Lee, P. Robison, P. Stergiou, and S. Kim. "Malicious Firmware Detection with Hardware Performance Counters". In: *IEEE Transactions on Multi-Scale Computing Systems* 2.3 (2016), pp. 160–173

[J10] N.G. Tsoutsos and M. Maniatakos. "The HEROIC Framework: Encrypted Computation without Shared Keys". In: *Special Issue of IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34.6 (2015), pp. 875–888

[J9] M. Maniatakos, M. Michael, and Y. Makris. "Multiple-Bit Upset Protection in Microprocessor Memory Arrays using Vulnerability-based Parity Optimization and Interleaving". In: *IEEE Transactions on VLSI* 23.11 (2015), pp. 2447–2460

[J8] M. Maniatakos, M. Michael, C. Tirumurti, and Y. Makris. "Revisiting Vulnerability Analysis in Modern Microprocessors". In: *IEEE Transactions on Computers* 64.9 (2015), pp. 2664–2674

[J7] 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* 2.1 (2014), pp. 81–93

[J6] 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

[J5] 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

[J4] 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

[J3] 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

[J2] 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

[J1] D. Gizopoulos, 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

Conference proceedings

[C56] D. Tychalas, H. Benkraouda, and M. Maniatakos. "ICSFuzz: Manipulating I/Os and Repurposing Binary Code to Enable Instrumented Fuzzing in ICS Control Applications". In: *USENIX Security*. 2021 (to appear)

[C55] E. Chielle, H. Gamil, and M. Maniatakos. "Real-time Private Membership Test using Homomorphic Encryption". In: *IEEE Design, Automation and Test in Europe (DATE)*. 2021 (to appear)

[C54] P. Rapjut, and M. Maniatakos. "Towards Non-intrusive Malware Detection for Industrial Control Systems". In: *IEEE Design, Automation and Test in Europe (DATE)*. 2021 (to appear)

[C53] A. Agrawal, M. Sazos, A. Al Durra, and M. Maniatakos. "Towards Robust Power Grid Attack Protection using LightGBM with Concept Drift Detection and Retraining". In: *ACM Workshop on Cyber Physical Systems and Internet of Things Security and Privacy (CPSIoTSec), co-located with CCS*. 2020, pp. 31–36

[C52] D. Tychalas and M. Maniatakos. "Potentially Leaky Controller: Examining Cache Side-Channel Attacks in Programmable Logic Controllers". In: *IEEE International Conference on Computer Design (ICCD)*. 2020 (to appear)

[C51] H. Gamil, P. Mehta, E. Chielle, A. Di Giovanni, M. Nabeel, F. Arneodo, and M. Maniatakos. "Muon-Ra: Quantum random number generation from cosmic rays". In: *IEEE International Online Testing Symposium (IOLTS)*. 2020, pp. 1–6

[C50] L. Hadjidemetriou, G. Tertytchny, H. Karbouj, C. Charalambous, M. Michael, M. Sazos, and M. Maniatakos. "Demonstration of Man in the Middle Attack on a Feeder Power Factor Correction Unit". In: *IEEE PES Innovative Smart Grid Technologies Europe (ISGT)*. 2020, pp. 126–130

[C49] E. Sarkar, H. Benkraouda, and M. Maniatakos. "I came, I saw, I hacked: Automated Generation of Process-independent Attacks for Industrial Control Systems". In: *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*. 2020, pp. 744–758

[C48] H. Benkraouda, M.A. Chakkantakath, A. Keliris, and M. Maniatakos. "SNIFU: Secure Network Interception for Firmware Updates in legacy PLCs". In: *IEEE VLSI Test Symposium (VTS)*. 2020, pp. 1–6

[C47] P. Rajput, P. Rajput, M. Sazos, and M. Maniatakos. "Process-Aware Cyberattacks for Thermal Desalination Plants". In: *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*. 2019, pp. 441–452

[C46] P. Rajput and M. Maniatakos. "JTAG: A Multifaceted Tool for Cyber Security". In: *IEEE International Online Testing Symposium (IOLTS)*. 2019, pp. 155–158

[C45] D. Tychalas, A. Keliris, and M. Maniatakos. "LED Alert: Supply Chain Threats for Stealthy Data Exfiltration in Industrial Control Systems". In: *IEEE International Online Testing Symposium (IOLTS)*. 2019, pp. 194–199

[C44] Esha Sarkar and Michail Maniatakos. "On automating delayered IC analysis for hardware IP protection". In: *ACM International Conference on Omni-Layer Intelligent Systems (COINS)*. 2019, pp. 205–210

[C43] M. Nabeel, M. Ashraf, E. Chielle, N.G. Tsoutsos, and M. Maniatakos. "CoPHEE: Co-processor for Partially Homomorphic Encrypted Execution". In: *IEEE Hardware-Oriented Security and Trust (HOST)*. 2019, pp. 131–140

[C42] C. Konstantinou, M. Sazos, and M. Maniatakos. "FLEP-SGS^2: a Flexible and Low-cost Evaluation Platform for Smart Grid Systems Security". In: *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. 2019, pp. 1–5

[C41] A. Keliris and M. Maniatakos. "ICSREF: A Framework for Automated Reverse Engineering of Industrial Control Systems Binaries". In: *Network and Distributed System Security Symposium (NDSS)*. 2019 (**Distinguished paper finalist**)

[C40] D. Tychalas and M. Maniatakos. "Open Platform Systems Under Scrutiny: A Cybersecurity Analysis of the Device Tree". In: *IEEE International Conference on Electronics Circuits and Systems (ICECS)*. 2018, pp. 477–480

[C39] A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos. "Low-budget Energy Sector Cyberattacks via Open Source Exploitation". In: *IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. 2018 (**Best paper award**)

[C38] C. Konstantinou, E. Chielle, and M. Maniatakos. "PHYLAX: Snapshot-based Profiling of Real-Time Embedded Devices via JTAG Interface". In: *IEEE Design, Automation and Test in Europe (DATE)*. 2018, pp. 869–872

[C37] N.G. Tsoutsos, O. Mazonka, and M. Maniatakos. "Memory-bounded Randomness for Hardware-constrained Encrypted Computation". In: *IEEE International Conference on Computer Design (ICCD)*. 2017, pp. 673–680

[C36] N.G. Tsoutsos and M. Maniatakos. "Obfuscating Branch Decisions based on Encrypted Data using MISR and Hash Digests". In: *IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. 2017, pp. 115–120

[C35] N. Gupta, F. Chen, N.G. Tsoutsos, and M. Maniatakos. "ObfusCADe: Obfuscating Additive Manufacturing CAD Models Against Counterfeiting". In: *ACM/EDAC/IEEE Design Automation Conference (DAC)*. 2017, pp. 1–6. DOI: 10:1145/3061639:3079847

[C34] N.G. Tsoutsos, H. Gamil, and M. Maniatakos. "Secure 3D Printing: Reconstructing and Validating Solid Geometries using Toolpath Reverse Engineering". In: *ACM Asia Conference on Computer and Communications Security, Workshop on Cyber-Physical Systems Security (CPSS)*. 2017, pp. 15–20

[C33] D. Tychalas, N.G. Tsoutsos, and M. Maniatakos. "SGXCrypter: IP Protection for Portable Executables using Intel's SGX Technology". In: *Asia and South Pacific Design Automation Conference (ASP-DAC)*. 2017, pp. 354–359

[C32] A. Keliris, H. Salehghaffari, B. Cairl, P. Krishnamurthy, M. Maniatakos, and F. Khorrami. "Machine Learning-based Defense Against Process-Aware Attacks on Industrial Control Systems". In: *IEEE International Test Conference (ITC)*. 2016, pp. 12.2.1–12.2.10

[C31] C. Konstantinou and M. Maniatakos. "A Case Study on Implementing False Data Injection Attacks Against Nonlinear State Estimation". In: *ACM Conference on Computer and Communications Security, Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC)*. 2016, pp. 81–92

[C30] A. Keliris and M. Maniatakos. "Remote Field Device Fingerprinting Using Device-Specific Modbus Information". In: *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*. 2016, pp. M1610–LC1.1–M1610–LC1.4 (Best student paper candidate - 3rd place)

[C29] N.G. Tsoutsos and M. Maniatakos. "Cryptographic Vote-Stealing Attacks Against a Partially Homomorphic E-voting Architecture". In: *IEEE International Conference on Computer Design (ICCD)*. 2016, pp. 157–160

[C28] C. Konstantinou, A. Keliris, and M. Maniatakos. "Taxonomy of Firmware Trojans in Smart Grid Devices". In: *IEEE Power and Energy Society General Meeting (PES)*. 2016. DOI: 10.1109/PESGM.2016.7741452

[C27] C. Konstantinou, M. Sazos, and M. Maniatakos. "Attacking the Smart Grid using Public Information". In: *IEEE Latin-American Test Symposium (LATS)*. 2016, pp. 105–110

[C26] A. Keliris, C. Konstantinou, N.G. Tsoutsos, R. Baiad, and M. Maniatakos. "Enabling Multi-Layer Cyber-Security Assessment of Industrial Control Systems through Hardware-in-the-Loop Testbeds". In: *Asia and South Pacific Design Automation Conference (ASP-DAC)*. 2016, pp. 511–518

[C25] N.G. Tsoutsos and M. Maniatakos. "Obfuscated Arbitrary Computation using Cryptographic Primitives". In: *IEEE International Design and Test Symposium (DTS)*. 2015, pp. 5–8

[C24] C. Konstantinou and M. Maniatakos. "Impact of Firmware Modification Attacks on Power Systems Field Devices". In: *IEEE International Conference on Smart Grid Communications (SMARTGRIDCOMM)*. 2015, pp. 283–288

[C23] A. Keliris, V. Dimitsas, O. Kremmyda, D. Gizopoulos, and M. Maniatakos. "Efficient parallelization of the Discrete Wavelet Transform algorithm using memory-oblivious optimizations". In: *International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS)*. 2015, pp. 25–32 (**Best paper award**)

[C22] X. Wang, C. Konstantinou, R. Karri, and M. Maniatakos. "ConFirm: Detecting Firmware Modifications in Embedded Systems using Hardware Performance Counters". In: *IEEE International Conference on Computer-Aided Design (ICCAD)*. 2015, pp. 544–551 (**Top Pick in Hardware and Embedded Security**)

[C21] N.G. Tsoutsos and M. Maniatakos. "Extending Residue-based Fault Tolerance to Encrypted Computation". In: *IEEE International Test Conference (ITC)*. 2015, pp. 23.3.1–23.3.10

[C20] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, and Y. Jin. "Cyber-Physical Systems: A Security Perspective". In: *IEEE European Test Symposium (ETS)*. 2015, pp. 1–8

[C19] C. Konstantinou, A. Keliris, and M. Maniatakos. "Privacy-Preserving Functional IP Verification utilizing Fully Homomorphic Encryption". In: *IEEE Design, Automation and Test in Europe (DATE)*. 2015, pp. 333–338

[C18] R. Kannavara, P. Schaumont, M. Maniatakos, M. Smith, and S. Buck. "Innovative Engineering Outreach Using Intel Security and Embedded Tools". In: *European Workshop on Microelectronics Education (EWME)*. 2014, pp. 127–132

[C17] N.G. Tsoutsos, C. Konstantinou, and M. Maniatakos. "Advanced Techniques for Designing Stealthy Hardware Trojans". In: *ACM/EDAC/IEEE Design Automation Conference (DAC)*. 2014, 174:1–174:4

[C16] N.G. Tsoutsos and M. Maniatakos. "HEROIC: Homomorphically EncRypted One Instruction Computer". In: *IEEE Design, Automation and Test in Europe (DATE)*. 2014, 246:1–246:6

[C15] N.G. Tsoutsos and M. Maniatakos. "Trust no one: Thwarting "heartbleed" attacks using privacy-preserving computation". In: *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 2014, pp. 59–64

[C14] A. Keliris and M. Maniatakos. "Investigating Large Integer Arithmetic on Intel Xeon Phi SIMD Extensions". In: *IEEE Design and Test of Integrated Systems (DTIS)*. 2014, pp. 1–6

[C13] 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 (SPACE)*. 2013, pp. 21–37

[C12] 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 (IOLTS)*. 2013, pp. 49–54

[C11] M. Maniatakos. "Privilege escalation attack through address space identifier corruption in untrusted modern processors". In: *IEEE Design and Technology of Integrated Systems (DTIS)*. 2013, pp. 161–166

[C10] 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 (DATE)*. 2013, pp. 1480–1485

[C9] M. Maniatakos, M. Michael, and Y. Makris. "Vulnerability-Based Interleaving for Multi-Bit Upset (MBU) Protection in Modern Microprocessors". In: *IEEE International Test Conference (ITC)*. 2012, pp. 19.2.1–19.2.8

[C8] Y. Jin, M. Maniatakos, and Y. Makris. "Exposing vulnerabilities of untrusted computing platforms". In: *IEEE International Conference on Computer Design (ICCD)*. 2012, pp. 91–96

[C7] M. Maniatakos, C. Tirumurti, A. Jas, and Y. Makris. "AVF Analysis Acceleration via Hierarchical Fault Pruning". In: *IEEE European Test Symposium (ETS)*. 2011, pp. 87–92

[C6] 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 (VTS)*. 2011, pp. 235–240

[C5] M. Maniatakos and Y. Makris. "Workload-driven selective hardening of control state elements in modern microprocessors". In: *IEEE VLSI Test Symposium (VTS)*. 2010, pp. 159–164

[C4] 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 (VTS)*. 2009, pp. 9–14

[C3] 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 (ICCD)*. 2009, pp. 91–96

[C2] 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 (DFTS)*. 2008, pp. 454–462

[C1] N. Karimi, M. Maniatakos, Y. Makris, and A. Jas. "On the correlation between Controller Faults and Instruction-Level Errors in Modern Microprocessors". In: *IEEE International Test Conference (ITC)*. 2008, pp. 24.1.1–24.1.10

Magazines

[M2] D. Tychalas, E. Sarkar, P. Rajput, H. Benkraouda, and M. Maniatakos. "Standardization and Diversity in Industrial Control Systems: Fallacies and Pitfalls from a Cybersecurity Standpoint". In: *IEEE Technical Committee on Cyber-Physical Systems* 5.1 (2020), pp. 7–12

[M1] A. Keliris and M. Maniatakos. "Demystifying Advanced Persistent Threats for Industrial Control Systems". In: *Mechanical Engineering* 139.3 (2017), pp. 13–17 (Featured in cover)

Whitepapers

[W1] A. Keliris, C. Konstantinou, and M. Maniatakos. "GE Multilin SR Protective Relays Passcode Vulnerability". In: *BlackHat USA [Online]*. 2017

Published Theses

[T1] Michail Maniatakos. *Enhancing modern microprocessor resiliency through workload-cognizant, cross-layer, error impact analysis*. Yale University, 2012

GitHub Repositories

- CoPHEE: Co-processor for Partially Homomorphic Encrypted Encryption (HOST'19) 5/19
- ICSREF: Industrial Control Systems Reverse Engineering Framework (NDSS'19) 12/18
- FLEP-SGS2: A Flexible and Low-cost Evaluation Platform for Smart Grid Systems Security assessment (PES'19) 12/18
- E3: Encrypt-Everything-Everywhere is a framework providing C++ classes for supporting computation on private data 10/18
- TERMinatorSuite: A collection of privacy-preserving benchmarks (CAL'18) 6/17
- SGXCrypter: A crypter using Intel SGX technology (ASP-DAC'17) 7/16
- Cryptoleq: Compiler, emulator for an abstract machine for encrypted and unencrypted computation (TIFS'16) 12/15

Tutorials

'Homomorphic encryption and its application to privacy-preserving genotype imputation'

- **ACM Conference on Bioinformatics, Computational Biology, and Health Informatics (ACM BCB)**, Virtual Event 9/20

'Hack Me If You Can: Hands-on IoT Hacking'

- **IEEE Design and Automation Conference (DAC)**, San Fransisco, CA 6/18

'Privacy-preserving signal processing'

- **IEEE International Symposium on Signal Processing and Information Technology**, Abu Dhabi, UAE 12/15

Invited Lectures

TU Kaiserslautern (Erasmus Mondus Distinguished Lecture Series)

- EIT-EIS-566-V-7 Robust Digital Systems: Critical Infrastructure Cybersecurity 6/17

Aristotle University of Thessaloniki, Thessaloniki, Greece

- Seasonal School on Critical Infrastructure Cybersecurity 6/17

Invited Presentations

'Privacy in a globally interconnected world'

- **New York University Abu Dhabi Institute**, Abu Dhabi, UAE 11/20

'Hardware-based acceleration of homomorphic encryption'

- **New York University**, Brooklyn, NY 11/20
- **Texas A&M University**, College Station, TX 10/20

'Hardware-based solutions for critical infrastructure security'

- **University of Patras**, Patras, Greece 1/20
- **University of Delaware**, Newark, DE 5/19
- **Indian Institute of Technology Kharagpur**, Videoconference 4/18
- **Aalto University**, Helsinki, Finland 9/17
- **Technische Universitat Darmstadt**, Darmstadt, Germany 6/17
- **University of Texas at Dallas**, Richardson, TX 6/16
- **Stevens Institute of Technology**, Hoboken, NJ 11/16
- **Columbia University**, New York, NY 11/16
- **Stony Brook University**, Stony Brook, NY, 11/16
- **Yale University**, New Haven, CT 11/16

'Towards a general-purpose homomorphically encrypted microprocessor'

- **KU Leuven**, Brussels, Belgium, 6/19

- **Yale University**, New Haven, CT 6/19
- **MIT**, Cambridge, MA 5/19

'On the feasibility of clock synchronization cyberattacks on power grids'
- **ENISA workshop on interdependencies between OES and DSPs**, Brussels, Belgium 6/19

'Development of a scalable testbed for efficient cyber security assessment'
- **6th Arab-American Frontiers Symposium**, Kuwait City, Kuwait 11/18
- **7th Edition Cybersecurity for Energy and Utilities Conference**, Abu Dhabi, UAE 3/18
- **Metropolitan Transportation Authority (MTA) Headquarters**, New York, NY 12/17

'The challenges of/risks of failing to secure attack surfaces on cyber-asset endpoints'
- **PAS Webinar with Infosecurity Magazine**, Online 9/17

'Cryptoleq: A Heterogeneous Abstract Machine for Encrypted and Unencrypted Computation'
- **University of Central Florida**, Orlando, FL 9/16
- **University of Florida**, Gainesville, FL 9/16

'A hardware approach to privacy-preserving general-purpose computation'
- **Workshop on increasing assurance in commodity computer systems without new silicon trust anchors**, New York, NY 8/16

'Trust no one: Thwarting heartbleed attacks using privacy-preserving computation'
- **American University in Dubai**, Dubai, UAE 2/15
- **International Conference in Secure Knowledge Management**, Dubai, UAE 10/14

'Cybersecurity for the smart-grid: Manhattan Case Study'
- **10th Carnegie Mellon Conference on the Electricity Industry**, Pittsburgh, PA 4/15
- **Office of Naval Research workshop**, Philadelphia, PA 3/15
- **Office of Naval Research workshop**, Santa Barbara, CA 1/15
- **Caxton ICS Cyber Defense for Energy**, Abu Dhabi, UAE 9/14

'Design and technology for a safer cyberspace'
- **University of Athens**, Greece 3/15
- **University of Piraeus**, Greece 3/15
- **Athens University of Economy and Business**, Greece 3/15

'An exploration of vector-based integer arithmetic on Intel Xeon Phi SIMD Extensions'
- **IEEE VLSI Test Symposium (VTS)**, Napa Valley, CA 4/14

'NYU Abu Dhabi Engineering: An Integrated Differentiated Curriculum for the 21st Century Engineer'
- **Informational Event for Educators**, Mexico City, Mexico 3/14
- **Informational Session for Parents**, Queretaro, Mexico 3/14

'Platform Profiling in Legacy Power Grid and Emerging Smart Grid Environment'
- **Consolidated Edison**, New York, NY 1/14

'Enabling Secure Computation on the Cloud'

- **Research Workshop on Emerging Data Center and Cloud Computing Technologies**, UAEU University, Abu Dhabi, UAE 12/13

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

- **Petroleum Institute**, Abu Dhabi, UAE 11/13

'Investigating the Application of OISC for Encrypted Computation'

- **Army Research Office Workshop on Trustworthy Hardware**, New York, NY 11/13
- **Columbia University**, New York, NY 9/13
- **IEEE International Test Conference (ITC)**, Anaheim, CA 9/13
- **IBM T.J. Watson**, Yorktown Heights, NY 9/13

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

- **IEEE VLSI Test Symposium (VTS)**, Berkeley, CA 4/13

'Robust and secure microprocessors'

- **IBM T.J. Watson**, Yorktown Heights, NY 7/12

'Enhancing robustness in modern microprocessors'

- **New York University Abu Dhabi**, Abu Dhabi, UAE 5/12
- **University of Texas at Dallas**, Richardson, TX 4/12
- **Polytechnic Institute of NYU**, New York, NY 4/12
- **Brown University**, Providence, RI 2/12

'Concurrent error detection in modern microprocessors'

- **Intel Corporation**, Santa Clara, CA 5/09

'Fault injection infrastructure for the Alpha 21264 processor'

- **Intel Corporation**, Santa Clara, CA 1/08

Institutional & Departmental Service

New York University

- Tenured/Tenure-Track Faculty Senator Global Network University Committee '17–'19

New York University Abu Dhabi

- Academic Integrity Committee '19–
- Dean of Arts and Humanities Search Committee '19–'20
- Tenured/Tenure-Track Faculty Senator '17–'19
- Engineering Graduate Committee '13–'20
  - Chair '16–'20
- Science and Engineering Curriculum Committee '16–'18
- Computer Engineering Program Coordinator '14–'18
- Faculty Council Steering Committee '14–'16
- Core Curriculum Committee '14–'15
- Campus Life and Faculty Liaison Committee '13–'15
- Annual Research Conference Engineering Program Committee '14–'15

New York University Tandon School of Engineering

- Faculty Program Curriculum Committee, Computer Engineering '14–'18

Community Service

New York University Abu Dhabi

- Robotics Club for kids 12-15, IdeaLab, NYU Abu Dhabi 2/15–6/15
- Robotics Workshop, Expo 2020 YouthConnect 11/15

New York University Tandon School of Engineering

- Faculty mentor for Embedded Security Challenge, CSAW '15–'19

Professional Service

Book Editor:

- 'VLSI-SoC: Opportunities and Challenges Beyond the Internet of Things', Springer, Editors: M. Maniatakos, I. M. Elfadel, M. Sonza Reorda, F. Ugurdag, J. Monteiro, R. Reis '18

Guest Associate Editor:

- IEEE Embedded Systems Letters: Special Issue on Embedded Security Challenge '17
- IEEE Design and Test: Special Issue on Cyber-Physical Systems Security and Privacy. Volume: 34, Issue: 4 8/17

Workshop Organizer:

- Joint Workshop on CPS&IoT Security and Privacy (CPSIoTSec), in conjunction with ACM CCS 2020 11/20
- NYUAD Center for Cyber Security Systems Security Brainstorming Workshop 11/18
- Office of Naval Research outreach for TCPC 8/16
- Army Research Office Workshop on Trustworthy Hardware 11/14
- 2nd 'Do You Trust Your Chip?' Workshop: Protecting the new generation of processing architectures 4/13

Panelist:

- Artificial Intelligence Hardware Systems Forum, Khalifa University, UAE 2/20
- IEEE International Verification and Security Workshop (IVSW), Security Concerns of Machine Learning and AI Systems 7/19
- Dubai World Government Summit, Roundtable on Artificial Intelligence 2/18
- UAE Security Forum, 'Bridging the Cybersecurity Talent Gap' 2/16
- National Science Foundation (NSF): Secure and Trustworthy Cyberspace (SaTC)

Advisory board:

- Pan-European Network of Practitioners in the field of Critical Infrastructures, International Advisory Board Member '17–

General Chair:

- IEEE International Conference on Computer Design (ICCD) (Co-Chair: O. Sinanoglu) '19

Program Chair:

- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) (Co-Chair: M. Sonza Reorda, Politecnico di Torino, Italy) '17

Program Track Chair:

- IEEE Computer Society Annual Symposium on VLSI (ISVLSI), System Design and Security Track '20
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Hardware Security Track (Co-Chair: L. Bossuet, University St. Etienne, France) '16, '18

- IEEE European Test Symposium (ETS), Security Track '17–'18
- IEEE International Conference on Computer Design (ICCD), Computer Systems and Architecture Track (Co-chair: E, Kursun, Columbia University, USA) '17
- IEEE International Conference on Computer Design (ICCD), Test, Verification and Security Track (Co-chair: J. Liou, National Tsing Hua University, Taiwan) '16

Special Session Organizer:
- IEEE International Conference on Computer Design (ICCD), Special Session on Embedded Security Challenge '16
- Design and Automation Conference (DAC), Special Session on Embedded Security Challenge '14

Local Arrangements Chair:
- IEEE International Conference on Computer Design (ICCD) '15
- IEEE International Symposium on Defect and Fault Tolerance in VLSI (DFT) '13
- IEEE International Symposium on Nanoscale Architectures (NANOARCH) '13

Proceedings/Publications Chair:
- IEEE On-line Testing Symposium (IOLTS) '15–'18
- ACM Asia Conference on Computer and Communications Security (AsiaCCS) '16

Tutorials Chair:
- IEEE International Workshop on Information Forensics and Security (WIFS) '16

Publicity Chair:
- IEEE International Conference on Computer Design (ICCD) '16

Session Chair/Moderator:
- IEEE On-line Testing Symposium (IOLTS) '15, '19
- IEEE Design, Automation and Test in Europe (DATE) '19
- Design and Automation Conference (DAC) '14, '16
- IEEE International Workshop on Information Forensics and Security (WIFS) '16
- Asia and South Pacific Design Automation Conference (ASP-DAC) '16
- IEEE International Conference on Computer Design (ICCD) '12, '15
- IEEE International Test Conference (ITC) '14
- NYU Abu Dhabi Research Conference '14
- IEEE VLSI Test Symposium (VTS) '13–'14
- Army Research Office Workshop on Trustworthy Hardware, NY '13
- International Conference on Security, Privacy and Cryptography Engineering (SPACE) '13

Technical Program Committee member:
- USENIX Security Symposium '21
- IEEE Design, Automation and Test in Europe (DATE) '20–'21
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) '16–'20
- IEEE International Conference on Compilers, Architectures, and Synthesis of Embedded Systems (CASES) '15–'20
- IEEE Asia Pacific Conference on Circuits and Systems (APCCAS) '20

- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) '17–'20
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) '18–'20
- IEEE On-line Testing Symposium (IOLTS) '16–'20
- Euromicro Conference on Digital System Design (DSD) '20
- IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) '19–'20
- Workshop on Binary Analysis Research (BAR), Network and Distributed System Security Symposium (NDSS) '20
- Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS 2020) '20
- IEEE Asian Hardware Oriented Security and Trust Symposium (AsiaHOST) '16–'20
- ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC) '15–'19
- ACS/IEEE International Conference on Computer Systems and Applications (AICCSA) '19
- IEEE Latin American Test Symposium (LATS) '18–'19
- IEEE International Symposium on VLSI (ISVLSI) '14–'19
- IEEE VLSI Test Symposium (VTS) '18
- ACM Asia Conference on Computer and Communications Security (AsiaCCS) '17–'18
- IEEE European Test Symposium (ETS) '17–'18
- IEEE International Test Conference (ITC) '14–'18
- ACM Cyber-Physical System Security Workshop (CPSS) '17–'18
- IEEE Cyber Science and Technology Congress (CyberSciTech) '18
- IEEE International Conference on Computer Design (ICCD) '12–'17
- IEEE North Atlantic Test Workshop (NATW) '16–'17
- IEEE Design and Automation Conference (DAC) '15–'16
- IEEE Design and Technology of Integrated Systems (DTIS) '13–'16
- ACM/IEEE Great Lakes Symposium on VLSI (GLSVLSI) '15–'16
- IEEE International Conference on Computer-Aided Design (ICCAD) '15–'16
- International Conference on Security, Privacy and Cryptography Engineering (SPACE) '14
- IEEE International Symposium on Defect and Fault Tolerance in VLSI (DFT) '12

Technical referee:

- ACM Computing Surveys
- ACM Transactions on Embedded Computing Systems
- ACM Journal of Emerging Technologies in Computing
- ACM Transactions on Design Automation of Electronic Systems
- IEEE Communication Letters
- IEEE Computer
- IEEE Consumer Electronics Magazine
- IEEE Design & Test
- IEEE Embedded Systems Letters
- IEEE Journal of Electronic Testing
- IEEE Open Journal of Power Electronics
- IEEE Security and Privacy
- IEEE Transactions on CAD
- IEEE Transactions on Circuits and Systems II: Express Briefs
- IEEE Transactions on Computers

- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Device and Materials Reliability
- IEEE Transactions on Emerging Topics in Computing
- IEEE Transactions on Industrial Informatics
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Multi-Scale Computing Systems
- IEEE Transactions on Nanotechnology
- IEEE Transactions on Parallel and Distributed Systems
- IEEE Transactions on VLSI
- Proceedings of the IEEE
- Springer Journal of Hardware and Systems Security
- Top Picks in Hardware and Embedded Security