

# Farinaz Koushanfar

University of California, San Diego  
9500 Gilman Drive, Mail Code 0407  
La Jolla, CA 92093-0407  
Citizenship: United States

farinaz@ucsd.edu  
Phone: +1-858-534-3294  
Fax: +1-858-534-5909  
<http://eceweb.ucsd.edu/~fkoushanfar>

## Education

<b>Ph.D. in Electrical Engineering and Computer Science</b> <i>University of California, Berkeley</i>	12/2005
<b>M.A. in Statistics</b> <i>University of California, Berkeley</i>	5/2005
<b>M.S. in Electrical Engineering (thesis jointly done in Computer Science)</b> <i>University of California, Los Angeles</i>	12/2000
<b>B.S. in Electrical Engineering</b> <i>Sharif University of Technology, Tehran, Iran</i>	12/1998

## Professional Experience

<b>Co-director of Machine-Integrated Computing and Security Center (MISC)</b> <i>University of California San Diego</i>	10/2018-Present
<b>Professor and Henry Booker Faculty Scholar</b> <i>University of California San Diego (UCSD), Electrical &amp; Computer Engineering</i>	11/2015-Present
<b>Professor</b> <i>Rice University, Electrical &amp; Computer Engineering</i>	09/2015-12/2015
<b>Associate Partner</b> <i>Intel Collaborative Research Institute for Secure Computing</i>	07/2014-Present
<b>Principal Director, Texas Instruments (TI) DSP Leadership</b> <i>Rice University</i>	09/2008-12/2015
<b>Assistant Professor and (Tenured) Associate Professor</b> <i>Rice University, Electrical &amp; Computer Engineering</i>	07/2006-09/2015
<b>Visiting Assistant Professor</b> <i>MIT Computer Science and Artificial Intelligence Laboratory (CSAIL)</i>	01/2010-07/2010
<b>Visiting Assistant Professor/ CSL Fellow</b> <i>Coordinated Science Lab (CSL), University of Illinois at Urbana-Champaign</i>	10/2005-07/2006
<b>Intel Open Collaborative Research Fellow</b> <i>Intel Research, Berkeley Lab</i>	08/2003-08/2004

## Awards and Honors

Fellow of IEEE . . . . .	2019
Best Student Paper Award, Field-Programmable Custom Computing Machines (FCCM) . . . . .	2018
ICCAD Ten Year Retrospective Most Influential Paper Award . . . . .	2018
Henry Booker Faculty Scholarship, UCSD . . . . .	2016
Cisco IoT Security Grand Challenge Award . . . . .	2014
National Academy of Science (NAS) Kavli Foundation Fellowship . . . . .	2012
Army Research Office (ARO) Young Investigator Program (YIP) Award . . . . .	2012
ACM SIGDA Outstanding New Faculty Award (ONFA) . . . . .	2011
Presidential Early Career Award for Scientists and Engineers (PECASE) . . . . .	2010
Office of Naval Research (ONR) Young Investigator Program (YIP) Award . . . . .	2009-2012
National Science Foundation (NSF) CAREER Award . . . . .	2007-2011
Young Faculty Award, Defense Advanced Research Projects Agency (DARPA) . . . . .	2007-2009
MIT Technology Review TR-35 Award (World's Top Innovators Under 35) . . . . .	2008
Cyber Security Awareness (CSAW) Best Applied Security Paper Award, 2nd place . . . . .	2013

National Academy of Engineering (NAE) “Frontiers of Engineering” . . . . .	2009
INTEL Open Collaborative Research (OCR) Fellowship Award . . . . .	2003-2004
Best Student Paper Award, ACM SIGMOBILE (Mobicom) . . . . .	2001
National Science Foundation (NSF) Graduate Student Research Fellowship . . . . .	2000-2003

<b>Publications list</b>
--------------------------

• **Peer-Reviewed Journal Articles**

35. S. U. Hussain and F. Koushanfar, “P3: Privacy Preserving Positioning for Smart Automotive Systems”, *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 23, issue 6, 2018.
34. S. U. Hussain, M. S. Riazi, and F. Koushanfar, “SHAIP: Secure Hamming Distance for Authentication of Intrinsic PUFs”, *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 23, issue 6, 2018.
33. M. S. Riazi, M. Samragh, and F. Koushanfar, “CAMsure: Secure Content-Addressable Memory for Approximate Search”, *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 5s, p. 136, 2017.
32. B. D. Rouhani, A. Mirhoseini, and F. Koushanfar, “RISE: An Automated Framework for Real-Time Intelligent Video Surveillance on FPGA”, *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 5s, p. 158, 2017.
31. M. S. Riazi, E. Songhori, A. - R. Sadeghi, T. Schneider, and F. Koushanfar, “Toward Practical Secure Stable Matching”, *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2017, issue 1, Jan 2017.
30. B. D. Rouhani, A. Mirhoseini, E. Songhori, and F. Koushanfar. “Automated Real-Time Analysis of Streaming Big and Dense Data on Reconfigurable Platforms.” *ACM Transactions on Reconfigurable Technology and Systems (TRETs)*, under minor revision for publication, 2016.
29. A. Mirhoseini, B. D. Rouhani, E. M. Songhori, and F. Koushanfar, “Chime: Checkpointing long computations on intermittently energized IoT devices,” *IEEE Transactions on Multi-Scale Computing Systems (TMSCS)*, vol. 2, issue 99, Jan 2016.
28. S. U. Hussain, M. Majzoobi, and F. Koushanfar, “A Built-In-Self-Test Scheme for Online Evaluation of Physical Unclonable Functions and True Random Number Generators,” *IEEE Transactions on Multi-Scale Computing Systems (TMSCS)*, vol. 2, no. 99, Jan 2016.
27. S. Chung, J. Kong, and F. Koushanfar, “An Energy-efficient Last-level Cache Architecture for Process Variation-tolerant 3D Microprocessors,” *IEEE Trans. on Computers*, vol. 64, no. 9, pp. 2460–2475, Sept 2015.
26. A. Mirhoseini, M. Potkonjak, and F. Koushanfar, “Phase Change Memory Write Cost Minimization by Data Encoding,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS), Special Issue on Computing in Emerging Technologies*, vol. 5, no. 1, pp. 51–63, Mar 2015.
25. A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, “Novel Techniques for High-sensitivity Hardware Trojan Detection using Thermal and Power Maps,” *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, vol. 33, no. 12, pp. 1792 – 1805, Dec 2014.
24. M. Rostami, F. Koushanfar, and R. Karri, “A Primer on Hardware Security: Models, Methods, and Metrics,” *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283 – 1295, Aug 2014.
23. C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,” *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug 2014.
22. J. Kong and F. Koushanfar, “Processor-based Strong Physical Unclonable Functions with Aging-based Response Tuning,” *IEEE Transactions on Emerging Topics in Computing (JETC)*, vol. 2, pp. 16–29, Mar 2014.
21. M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach, and S. Devadas, “Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching,” *IEEE Transactions on Emerging Topics in Computing (JETC)*, vol. 2, no. 1, pp. 37–49, Mar 2014.
20. A. Munir, A. Gordon-Ross, S. Ranka, and F. Koushanfar, “A Queueing Theoretic Approach for Performance Evaluation of Low-Power Multi-core Embedded Systems,” *Elsevier Journal of Parallel and Distributed Computing (JPDC)*, vol. 74, no. 1, pp. 1872 – 1890, Jan 2014.

19. A. Munir, F. Koushanfar, A. Gordon-Ross, and S. Ranka, "High-performance Optimizations on Tiled many-core Embedded Systems: A Matrix Multiplication Case Study," *The Journal of Supercomputing*, vol. 66, no. 1, pp. 431–487, Apr 2013.
18. Y.-K. Chen, A.-Y. Wu, M. A. Bayoumi, and F. Koushanfar, "Editorial: Low-power, Intelligent, and Secure Solutions for Realization of Internet of Things," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS)*, vol. 3, no. 1, pp. 1–4, Mar 2013.
17. N. Kiyavash, F. Koushanfar, T. P. Coleman, and M. Rodrigues, "A Timing Channel Spyware for the CSMA/CA Protocol," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 8, no. 3, pp. 477 – 487, Mar 2013.
16. M. Majzoobi, J. Kong, and F. Koushanfar, "Low-power Resource Binding by Postsilicon Customization," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 18, no. 2, p. 26:1–26:22, Mar 2013.
15. S. Wei, A. Nahapetian, M. Nelson, F. Koushanfar, and M. Potkonjak, "Gate Characterization using Singular Value Decomposition: Foundations and Applications," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 7, no. 2, pp. 765 – 773, Apr 2012.
14. F. Koushanfar, "Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 7, no. 1, pp. 51 – 63, Feb 2012.
13. F. Koushanfar and A. Mirhoseini, "A Unified Framework for Multimodal Submodular Integrated Circuits Trojan Detection," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 6, no. 1, pp. 162 –174, Mar 2011.
12. M. Majzoobi and F. Koushanfar, "Time-bounded Authentication of FPGAs," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 6, no. 3, pp. 1123–1135, Aug 2011.
11. J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending Piracy of Integrated Circuits," *IEEE Computer*, vol. 43, no. 10, pp. 30 – 38, Oct 2010.
10. F. Koushanfar, M. Majzoobi, and M. Potkonjak, "Nonparametric Combinatorial Regression for Shape Constrained Modeling," *IEEE Trans. On Signal Processing*, vol. 58, no. 2, pp. 626 – 637, Aug 2010.
9. M. Tehranipoor and F. Koushanfar, "Guest editors' introduction: Confronting the Hardware Trustworthiness Problem," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 8 – 9, Jan 2010.
8. M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," in *IEEE Design & Test of Computers*, vol. 27, no. 1, Jan 2010, pp. 10–25.
7. M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for Design and Implementation of Secure Reconfigurable PUFs," *ACM Trans. on Reconfigurable Technology and Systems (TRETs)*, vol. 2, no. 1, p. 5:1–5:33, Mar 2009.
6. F. Koushanfar, A. Davare, D.T. Nguyen, A.L. Sangiovanni-Vincentelli, and M. Potkonjak, "Techniques for Maintaining Connectivity in Wireless Ad-hoc Networks Under Energy Constraints," *ACM Trans. on Embedded Computing Systems (TECS)*, vol. 6, no. 3, 2007.
5. S. Megerian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Worst and Best-case Coverage in Sensor Networks," *IEEE Trans. on Mobile Computing*, vol. 4, pp. 84 – 92, Jan 2005.
4. F. Koushanfar, I. Hong, and M. Potkonjak, "Behavioral Synthesis Techniques for Intellectual Property Protection," *ACM Trans. Design Automation of Electronic Systems (TODAES)*, vol. 10, no. 3, pp. 523 – 545, Jul 2005.
3. J. Wong, F. Koushanfar, S. Megerian, and M. Potkonjak, "Probabilistic Constructive Optimization Techniques," *IEEE Trans. of Computer Aided Designs (TCAD)*, vol. 23, pp. 859–868, 2004.
2. S. Megerian, F. Koushanfar, G. Qu, G. Veltri, and M. Potkonjak, "Exposure in Wireless Sensor Networks: Theory and Practical Solutions," *ACM Journal of Wireless Networks*, vol. 8, pp. 443 – 454, Sep 2002.
1. F. Koushanfar, D. Kirovski, I. Hong, M. Potkonjak, and M. Papaefthymiou, "Symbolic Debugging of Embedded Hardware and Software," *IEEE Transactions on Computer-Aided Design*, vol. 20, pp. 392–401, Mar 2001.

- **Conference Proceedings**

115. B. D. Rouhani, H. Chen, and F. Koushanfar, "DeepSigns: An End-to-End Watermarking Framework for Protecting the Ownership of Deep Neural Networks," *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2019

114. S. U. Hussain, B. D. Rouhani, M. Ghasemzadeh, and F. Koushanfar, "MAXelerator: FPGA Accelerator for Privacy Preserving Multiply-Accumulate (MAC) on Cloud Servers," Design Automation Conference (DAC), 2018
113. M. S. Riazi, C. Weinert, O. Tkachenko, E. M. Songhori, T. Schneider, and F. Koushanfar, "Chameleon: A Hybrid Secure Computation Framework for Machine Learning Applications," Asia Conference on Computer and Communications Security (ASIACCS). ACM, 2018, pp. 707-721.
112. M. S. Riazi, B. D. Rouhani, and F. Koushanfar, "Deep Learning on Private Data," IEEE Security and Privacy (S&P) Magazine, 2018.
111. B. D. Rouhani, M. Ghasemzadeh, and F. Koushanfar, "CausaLearn: Automated Framework for Scalable Streaming-based Causal Bayesian Learning using FPGAs", International Symposium on Field-Programmable Gate Arrays (FPGA), 2018, pp. 1-10.
110. B. D. Rouhani, M. Samragh, M. Javaheripi, F. Koushanfar, and T. Javadi, "DeepFense: Online Accelerated Defense Against Adversarial Deep Learning", International Conference on Computer-Aided Design (ICCAD), 2018.
109. B. D. Rouhani, M. Samragh, T. Javadi, and F. Koushanfar, "Safe Machine Learning and Defeating Adversarial Attacks," IEEE Security and Privacy (S&P) Magazine, 2018.
108. M. Ghasemzadeh, M. Samragh, and F. Koushanfar, "ReBNet: Residual Binarized Neural Network," International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2018, pp. 57-64
107. B. D. Rouhani, M. S. Riazi, and F. Koushanfar, "DeepSecure: Scalable Provably-secure Deep Learning," Design Automation Conference (DAC), 2018.
106. H. Chen, S. Potluri, and F. Koushanfar, "BioChipWork: Reverse Engineering of Microfluidic Biochips," International Conference on Computer Design (ICCD), 2017, pp. 9-16.
105. M. S. Riazi, E. M. Songhori, and F. Koushanfar, "PriSearch: Efficient Search on Private Data," Design Automation Conference (DAC), 2017.
104. B. D. Rouhani, A. Mirhoseini, and F. Koushanfar, "Deep3: Leveraging Three Levels of Parallelism for Efficient Deep Learning," Design Automation Conference (DAC), 2017.
103. M. Samragh, M. Ghasemzadeh, and F. Koushanfar, "Customizing Neural Networks for Efficient FPGA Implementation," International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2017, pp. 85-92.
102. G. Dessouky, F. Koushanfar, A.R. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner, "Pushing the communication barrier in secure computation using lookup tables," Network and Distributed System Security Symposium (NDSS), 2017.
101. A. Mirhoseini, B. D. Rouhani, E. M. Songhori, and F. Koushanfar, "ExtDict: Extensible Dictionaries for Data- and Platform-Aware Large-Scale Learning," IEEE International Parallel & Distributed Processing Symposium (IPDPS), 2017.
100. B. D. Rouhani, A. Mirhoseini, and F. Koushanfar, "TinyDL: Just-In-Time Deep Learning Solution For Constrained Embedded Systems," International Symposium on Circuits and Systems (ISCAS), 2017.
99. M. Samragh, M. Imani, F. Koushanfar, and T. Rosing, "LookNN: Neural Network with No Multiplication," Design, Automation & Test in Europe (DATE), 2017.
98. B. D. Rouhani, A. Mirhoseini, and F. Koushanfar, "DeLight: Adding Energy Dimension To Deep Neural Networks," International Symposium on Low Power Electronics and Design (ISLPED), 2016, pp. 112-117.
97. B. D. Rouhani, A. Mirhoseini, and F. Koushanfar, "Going deeper than deep learning for massive data analytics under physical constraints," International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2016.
96. A. Mirhoseini, B. D. Rouhani, E. M. Songhori, and F. Koushanfar, "Perform-ML: Performance Optimized Machine Learning by Platform and Content Aware Customization," Design Automation Conference (DAC), 2016.
95. S. U. Hussain, and F. Koushanfar, "Privacy Preserving Localization for Smart Automotive Systems," Design Automation Conference (DAC), 2016.
94. E. M. Songhori, S. Zeitouni, G. Dessouky, T. Schneider, A. - R. Sadeghi, and F. Koushanfar, "GarbledCPU: A MIPS Processor for Secure Computation in Hardware," Design Automation Conference (DAC), 2016.
93. T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A. - R. Sadeghi, and G. Tsudik, "INVITED: Things, Trouble, Trust: On Building Trust in IoT Systems", Design Automation Conference (DAC), 2016.

92. Y. Zhang, and F. Koushanfar, "Robust Privacy-Preserving Fingerprint Authentication," IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016.
91. M. S. Riazzi, N. K. R. Dantu, V. L. N. Gattu, and F. Koushanfar, "GenMatch: Secure DNA Compatibility Testing", IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016.
90. A. Mirhoseini, A. - R. Sadeghi, and F. Koushanfar, "CryptoML: Secure Outsourcing of Big Data Machine Learning Applications," IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016.
89. F. Koushanfar, A. Mirhoseini, G. Qu, and Z. Zhang, "DA Systemization of Knowledge: A Catalog of Prior Forward-Looking Initiatives," (invited) International Conference on Computer-Aided Design (ICCAD), pp. 255–262 , 2015.
88. A. B. Kahng, and F. Koushanfar, "Evolving EDA Beyond its E-Roots: An Overview," (invited) International Conference on Computer-Aided Design (ICCAD), pp. 247-254, 2015.
87. E. Songhori, S.U. Hussain, A-R. Sadeghi, T. Schneider, and F. Koushanfar, "TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits," IEEE Symposium on Security and Privacy (S&P), pp. 411–428, 2015.
86. B. Rouhani, E. Songhori, A. Mirhoseini, and F. Koushanfar, "SSketch: An Automated Framework for Streaming Sketch-based Analysis of Big Data on FPGA", International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2015.
85. M. Miettinen, M. Sobhani, T.D. Nguyen, J. Rios, S. Yellapantula, N. Asokan, A-R. Sadeghi, and F. Koushanfar, "I Know Where You are: Proofs of Presence Resilient to Malicious Provers," ACM Symposium on Information, Computer and Communications Security (ASIACCS), pp. 567–577, 2015.
84. E. Songhori, S.U. Hussain, A-R. Sadeghi, and F. Koushanfar, "Compacting privacy-preserving k-nearest neighbor search using logic synthesis," Design Automation Conference (DAC), 2015.
83. E. Songhori, A. Mirhoseini, F. Koushanfar, "AHEAD: Automated Framework for Hardware Accelerated Iterative Data Analysis," Design, Automation & Test in Europe (DATE), pp. 942–947, 2015.
82. S. U. Hussain, S. Yellapantula, M. Majzoobi, and F. Koushanfar, "BIST-PUF: Online, Hardware-based Evaluation of Physically Unclonable Circuit Identifiers," International Conference on Computer-Aided Design (ICCAD), 2014, pp. 162–169.
81. D. Shahrjerdi, J. Rajendran, S. Garg, F. Koushanfar, and R. Karri, "Shielding and Securing Integrated Circuits with Sensors," International Conference on Computer-Aided Design (ICCAD), 2014, pp. 170–174.
80. J. Kong, F. Koushanfar, P. K. Pendyala, A.-R. Sadeghi, and C. Wachsmann, "PUFatt: Embedded Platform Attestation based on Novel Processor-based PUFs," Design Automation Conference (DAC) 2014, Best paper candidate.
79. M. Rostami, J. B. Wendt, M. Potkonjak, and F. Koushanfar, "Quo Vadis, PUF? Trends and Challenges of Emerging Physical-Disorder based Security," Design, Automation & Test in Europe (DATE), 2014, pp. 1–6.
78. A. Munir and F. Koushanfar, "D2Cyber: A Design Automation Tool for Dependable Cybercars," in Design, Automation & Test in Europe (DATE), 2014, pp. 1–4.
77. J. B. Wendt, F. Koushanfar, and M. Potkonjak, "Techniques for Foundry Identification," Design Automation Conference (DAC), 2014.
76. A. Munir, F. Koushanfar, H. Seudié, and A.-R. Sadeghi, "Cycar'2013: First international academic workshop on security, privacy and dependability for cybervehicles," ACM Conference on Computer & Communications Security (CCS), 2013, pp. 1481–1482.
75. M. Rostami, F. Koushanfar, J. Rajendran, and R. Karri, "Hardware Security: Threat Models and Metrics," International Conference on Computer-Aided Design (ICCAD), 2013, pp. 819–823.
74. M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-Heart (H2H): Authentication for Implanted Medical Devices," ACM Conference on Computer & Communications Security (CCS), 2013, pp. 1099–1112.
73. Y. Yao, M.-B. Kim, J. Li, I. L. Markov, and F. Koushanfar, "ClockPUF: Physical Unclonable Functions based on Clock Networks," Design, Automation & Test in Europe (DATE), 2013, pp. 422–427.
72. K. Hu, A. N. Nowroz, S. Reda, and F. Koushanfar, "High-sensitivity Hardware Trojan Detection using Multimodal Characterization," in Design, Automation & Test in Europe (DATE), 2013, pp. 1271 – 1276.

71. A. Mirhoseini, E. M. Songhori, and F. Koushanfar, "Idetic: A High-level Synthesis Approach for enabling Long Computations on Transiently-powered ASICs," *Pervasive Computing and Communication conference (PerCom)*, 2013, pp. 216–224.
70. A. Mirhoseini, E. M. Songhori, and F. Koushanfar, "Automated Checkpointing for Enabling Intensive Applications on Energy Harvesting Devices," *International Symposium on Low Power Electronics and Design (ISLPED)*, 2013, pp. 27–32.
69. M. Rostami, W. Burlison, A. Juels, and F. Koushanfar, "Balancing Security and Utility in Medical Devices?" *Design Automation Conference (DAC)*, 2013.
68. S. Wei, K. Li, F. Koushanfar, and M. Potkonjak, "Provably Complete Hardware Trojan Detection using Test Point Insertion," *International Conference on Computer-Aided Design (ICCAD)*, 2012, pp. 51–63.
67. F. Koushanfar, S. Fazzari, C. McCants, W. Bryson, M. Sale, P. Song, and M. Potkonjak, "Can EDA Combat the rise of Electronic Counterfeiting?" *Design Automation Conference (DAC)*, 2012.
66. A. Mirhoseini, M. Potkonjak, and F. Koushanfar, "Coding-based Energy Minimization for Phase Change Memory," *Design Automation Conference (DAC)*, 2012.
65. F. Koushanfar, A.-R. Sadeghi, and H. Seudie, "EDA for Secure and Dependable Cybercars: Challenges and Opportunities," *Design Automation Conference (DAC)*, 2012.
64. S. Wei, K. Li, F. Koushanfar, and M. Potkonjak, "Hardware Trojan Horse Benchmark via Optimal Creation and Placement of Malicious Circuitry," *Design Automation Conference (DAC)*, 2012.
63. M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching," *International Workshop on Trustworthy Embedded Devices (TrustED)*, 2012, pp. 33–44.
62. F. Koushanfar and A. Mirhoseini, "Hybrid Heterogeneous Energy Supply Networks," *International Symposium on Circuits and Systems (ISCAS)*, 2011, pp. 2489–2492.
61. E. Dyer, M. Majzoobi, and F. Koushanfar, "Hybrid Modeling of Non-stationary Process Variations," *Design Automation Conference (DAC)*, 2011.
60. A. Mirhoseini and F. Koushanfar, "Hypoenergy: Hybrid Supercapacitor-battery Power-supply Optimization for Energy Efficiency," *Design, Automation & Test in Europe (DATE)*, 2011, pp. 887–890.
59. S. Wei, F. Koushanfar, and M. Potkonjak, "Integrated Circuit Digital Rights Management Techniques using Physical Level Characterization," *ACM workshop on Digital rights management (DRM)*, 2011, pp. 3–14.
58. F. Koushanfar, "Integrated Circuits Metering for Piracy Protection and Digital Rights Management: An Overview," *ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2011, Invited Paper, pp. 449–454.
57. A. Mirhoseini and F. Koushanfar, "Learning to Manage Combined Energy Supply Systems," *International Symposium on Low Power Electronics and Design (ISLPED)*, 2011, pp. 229–234.
56. M. Majzoobi, G. Ghiaasi-Hafezi, F. Koushanfar, and S. Nassif, "Ultra-low Power Current-based PUF," *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2011, pp. 2071–2074.
55. M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA PUF using Programmable Delay Lines," *IEEE Workshop on Information Forensics and Security*, 2010, pp. 1–6.
54. F. Koushanfar, "Hierarchical Hybrid Power Supply Networks," *Design Automation Conference (DAC)*, 2010.
53. F. Koushanfar and Y. Alkabani, "Provably Secure Obfuscation of Diverse Watermarks for Sequential Circuits," *International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2010, pp. 42–47.
52. M. Majzoobi, E. Dyer, A. Elnably, and F. Koushanfar, "Rapid FPGA Characterization using Clock Synthesis and Signal Sparsity," *International Test Conference (ITC)*, 2010, pp. 457–466.
51. A. Mirhoseini, Y. Alkabani, and F. Koushanfar, "Real Time Emulations: Foundation and Applications," in *Design Automation Conference (DAC)*, 2010.
50. Y. Alkabani and F. Koushanfar, "Consistency-based Characterization for IC Trojan Detection," *International Conference on Computer Aided Design (ICCAD)*, 2009, pp. 123–127.
49. F. Koushanfar and D. Shamsi, "The Challenges of Model Objective Selection and Estimation for Ad-hoc Network Data Sets," *Institute of Mathematical Statistics (IMS) Lecture Notes-Monograph Series (LNMS)*, vol. 57, pp. 332–345, 2009.
48. Y. Alkabani, F. Koushanfar, and M. Potkonjak, "N-version Temperature-aware Scheduling and Binding," *International Symposium on Low Power Electronics and Designs (ISLPED)*, 2009, pp. 331–334.

47. A. Candore, O. Kocabas, and F. Koushanfar, "Robust Stable Radiometric Fingerprinting for Wireless Devices," IEEE International Workshop on Hardware-Oriented Security and Trust (HOST), 2009, pp. 43–49.
46. Y. Alkabani, F. Koushanfar, N. Kiyavash, and M. Potkonjak, "Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach," Information Hiding (IH), 2008, pp. 102–117.
45. M. Potkonjak and F. Koushanfar, "(Bio)-behavioral CAD," Design Automation Conference (DAC), 2008.
44. Y. Alkabani and F. Koushanfar, "Active Control and Digital Rights Management of Integrated Circuit IP Cores," in Compilers, Architectures, and Synthesis for Embedded Systems (CASES), 2008.
43. J. Roy, F. Koushanfar, and I. Markov, "Epic: Ending Piracy of Integrated Circuits," Design Automation & Test in Europe (DATE), 2008.
42. Y. Alkabani, T. Massey, F. Koushanfar, and M. Potkonjak, "Input Vector Control for Post-Silicon Leakage Current Minimization in the Presence of Manufacturing Variability," Design Automation Conference (DAC), 2008.
41. M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight Secure PUFs," International Conference on Computer-Aided Design (ICCAD), 2008, pp. 670–673.
40. Y. Alkabani and F. Koushanfar, "N-variant IC Design: Methodology and Applications," Design Automation Conference (DAC), 2008.
39. D. Shamsi, P. Boufounos, and F. Koushanfar, "Noninvasive Leakage Power Tomography of Integrated Circuits by Compressive Sensing," International symposium on Low power electronics and design (ISLPED), 2008, pp. 341–346.
38. F. Koushanfar, P. Boufounos, and D. Shamsi, "Post-silicon Timing Characterization by Compressed Sensing," International Conference on Computer Aided Design (ICCAD), 2008, pp. 185–189.
37. J. Roy, F. Koushanfar, and I. Markov, "Protecting Bus-based Hardware IP by Secret Sharing," Design Automation Conference (DAC), 2008.
36. M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing Techniques for Hardware Security," International Test Conference (ITC), 2008, pp. 1–10.
35. D. Shamsi, F. Koushanfar, and M. Potkonjak, "Challenging Benchmark for Location Discovery in Ad-hoc Networks," ACM international symposium on Mobile ad hoc networking and computing (MobiHoc), 2008, p. 361.
34. J. A. Roy, F. Koushanfar, and I. L. Markov, "Extended Abstract: Circuit CAD Tools as a Security Threat," IEEE International Workshop on Hardware-Oriented Security and Trust (HOST), 2008, pp. 65–66.
33. Y. Alkabani and F. Koushanfar, "Extended Abstract: Designer's Hardware Trojan Horse," IEEE International Workshop on Hardware-Oriented Security and Trust (HOST), 2008, pp. 82–83.
32. N. Kiyavash and F. Koushanfar, "Anti-collusion Position Estimation in Wireless Sensor Networks," IEEE Mobile Ad-hoc and Sensor Systems (MASS), 2007.
31. F. Koushanfar and M. Potkonjak, "CAD-based Security, Cryptography, and Digital Rights Management," Design Automation Conference (DAC), 2007.
30. F. Koushanfar and M. Potkonjak, "A General Framework for Spatial Correlation Modeling in VLSI Design," in Design Automation Conference (DAC), 2007.
29. F. Koushanfar and M. Potkonjak, "Hardware Security: Preparing Students for the Next Design Frontiers," IEEE International Conference on Microelectronic Systems Education (MSE), 2007.
28. F. Koushanfar, M. Potkonjak, "Integration of Statistical Techniques in the Design Curriculum," IEEE International Conference on Microelectronic Systems Education (MSE), 2007, pp. 153–154.
27. S. So, F. Koushanfar, A. Kosterev, and F. Tittel, "Laserspecks: Laser Spectroscopic Trace-gas Sensor Networks - Sensor Integration and Applications," Information Processing in Sensor Networks (IPSN), 2007, pp. 226–235.
26. Y. Alkabani, F. Koushanfar, and M. Potkonjak, "Remote Activation of ICs for Piracy Prevention and Digital Right Management," International Conference on Computer Aided Design (ICCAD), 2007, pp. 674–677.
25. F. Koushanfar, A. Daware, D. Nguyen, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Techniques for Maintaining Connectivity Ad-hoc Networks under Energy Constraints," ACM Transaction on Embedded Computing Systems (TECS), vol. 6, 2007, pp. 16–16.

24. Y. Alkabani and F. Koushanfar, "Active Hardware Metering for Intellectual Property Protection and Security," in *USENIX Security Symposium*, 2007, pp. 291–306.
23. F. Koushanfar and M. Potkonjak, *Watermarking Technique for Sensor Networks: Foundations and Applications*. CRC Press, 2006.
22. F. Koushanfar, N. Kiyavash, and M. Potkonjak, "Interacting Particle-based Model for Missing Data in Sensor Networks: Foundations and Applications," *IEEE Sensors*, 2006, pp. 888–891.
21. F. Koushanfar, N. Taft, and M. Potkonjak, "Sleeping Coordination for Comprehensive Sensing using Isotonic Regression and Domatic Partitions," *IEEE International Conference on Computer Communications (INFOCOM)*, 2006, pp. 1–13.
20. J. Wong, F. Koushanfar, and M. Potkonjak, "Flexible ASICs: Shared Masking for Multiple Media Processors," *Design Automation Conference (DAC)*, 2005.
19. F. Koushanfar and M. Potkonjak, "Markov Chain-based Models for Missing and Faulty Data in Mica2 Sensor Motes," *IEEE Sensors*, 2005, pp. 1430–1434.
18. F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Error Models for Light Sensors by Statistical Analysis of Raw Sensor Measurements," *IEEE Sensors*, vol. 2, Oct 2004, pp. 1472–1475.
17. F. Koushanfar, A. Davare, D. Nguyen, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Low Power Coordination in Wireless Ad-hoc Networks," *International Symposium on Low Power Electronics and Design (ISLPED)*, 2003, pp. 475–480.
16. F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli, "On-line Fault Detection of Sensor Measurements," *IEEE Sensors*, vol. 2, Oct 2003, pp. 974–979.
15. F. Koushanfar, S. Slijepcevic, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Error-tolerant Multi-modal Sensor Fusion," *IEEE CAS Workshop on Wireless Communications and Networking*, 2002.
14. F. Koushanfar, J. Wong, J. Feng, and M. Potkonjak, "IIP-based Engineering Change," *Design Automation Conference (DAC)*, 2002.
13. J. Feng, F. Koushanfar, and M. Potkonjak, "System-architectures for Sensor Networks Issues, Alternatives, and Directions," *International Conference of Computer Design (ICCD)*, 2002, pp. 226–231.
12. F. Koushanfar, S. Slijepcevic, J. Wong, and M. Potkonjak, "Global Error-tolerant Algorithms for Location Discovery in Ad-hoc Wireless Networks," *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, 2002, pp. IV–4186 – IV–4186.
11. F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Fault Tolerance Techniques for Wireless Ad-hoc Sensor Networks," *IEEE Sensors*, vol. 2, 2002, pp. 1491–1496.
10. S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in Wireless Ad-hoc Sensor Networks," *International conference on Mobile computing and networking (MobiCom)*, 2001, pp. 139–150.
9. F. Koushanfar and G. Qu, "Hardware Metering," *Design Automation Conference (DAC)*, 2001.
8. F. Koushanfar, G. Qu, and M. Potkonjak, "Intellectual property metering," *Information Hiding Workshop (IHW)*, 2001, pp. 81–95.
7. J. Wong, F. Koushanfar, S. Meguerdichian, and M. Potkonjak, "A Probabilistic Constructive Approach to Optimization Problems," *International Conference on Computer Aided Design (ICCAD)*, 2001, pp. 453–456.
6. S. Meguerdichian, F. Koushanfar, A. Morge, D. Petranovic, and M. Potkonjak, "Metacores: Design and Optimization Techniques," *Design Automation Conference (DAC)*, 2001.
5. S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Coverage Problems in Wireless Ad-hoc Sensor Networks," *IEEE International Conference on Computer Communications (INFOCOM)*, vol. 3, 2001, pp. 1380–1387.
4. J. Rabaey, M. Potkonjak, F. Koushanfar, S. Li, and T. Tuan, "Challenges and Opportunities in Broadband and Wireless Communication Designs," *International Conference on Computer Aided Design (ICCAD)*, 2000, pp. 76–82.
3. F. Koushanfar, V. Prabhu, M. Potkonjak, and J. Rabaey, "Processors for Mobile Applications," *International Conference on Computer Designs (ICCD)*, 2000, pp. 603–608.
2. F. Koushanfar, D. Kirovski, and M. Potkonjak, "Symbolic Debugging Scheme for Optimized Hardware and Software," *International Conference on Computer Aided Design (ICCAD)*, 2000, pp. 40–43.
1. A. E. Caldwell, Y. Cao, A. B. Kahng, F. Koushanfar, H. Lu, I. L. Markov, M. Oliver, D. Stroobandt, and D. Sylvester, "GTX: The Marco GSRC Technology Extrapolation System," *Design Automation Conference (DAC)*, 2000.



- **Book Chapters**

10. U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, M. Majzoobi, F. Koushanfar, and W. Burleson, *Efficient Power and Timing Side Channels for Physical Unclonable Functions*, ser. Lecture Notes in Computer Science/Cryptographic Hardware and Embedded Systems – CHES 2014, 2014, vol. 8731.
9. M. Majzoobi, F. Koushanfar, and S. Devadas, “FPGA-based True Random Number Generation using Circuit Metastability with Adaptive Feedback Control,” 2011, pp. 17–32.
8. M. Majzoobi, F. Koushanfar, and M. Potkonjak, *FPGA-oriented Security*, 2011.
7. F. Koushanfar, *Hardware Metering: A Survey.*, 2011.
6. U. Rührmair, S. Devadas, and F. Koushanfar, *Security based on Physical Unclonability and Disorder*, Springer 2011.
5. M. Majzoobi, A. Elnably, and F. Koushanfar, “FPGA Time-bounded Unclonable Authentication,” in *Information Hiding*, ser. Lecture Notes in Computer Science, vol. 6387, 2010, pp. 1 – 16.
4. F. Koushanfar, A. Mirhoseini, and Y. Alkabani, “A Unified Framework for Multimodal Submodular IC Trojan Detection,” in *Information Hiding Conference*, 2010, pp. 17–32.
3. M. Nelson, A. Nahapetian, F. Koushanfar, and M. Potkonjak, “SVD-based Ghost Circuitry Detection,” in *Information Hiding (IH)*, 2009, pp. 221 – 234.
2. F. Koushanfar, M. Potkonjak, and J. Feng, *Sensor Network Architecture*, 2005.
1. F. Koushanfar, S. Slijepcevic, M. Potkonjak, and A. Sangiovanni-Vincentelli, *Location Discovery in Ad-hoc Wireless Sensor Networks*, 2003.

<b>Professional Activities</b>
--------------------------------

- **Keynote Speaker (Invited)**

- Women in Hardware and Systems Security (WISE), co-located with Hardware-Oriented Security and Trust (HOST), 2017
- UCSD Jacobs School of Engineering Research Expo, 2017
- ACM Workshop on Scalable Trusted Computing (ACM STC), co-located with ACM Conference on Computer and Communications Security (CCS), 2011

- **Associate Editor**

- IEEE Transactions on Dependable and Secure Computing (TDSC), 2018-Present
- IEEE Transactions on Information Forensics and Security, 2012-2016
- IEEE Transactions on Very Large Scale Integration Systems (VLSI), 2009-2011
- Ad-Hoc Networks Journal (Elsevier), 2010-2014

- **Guest Editor**

- ACM Transactions on Design Automation of Electronic Systems (TODAES), Special issue on IoT Security, 2018
- IEEE Transactions on Computer-Aided Design (TCAD), Hardware Security and Trust, 2015
- Proceedings of IEEE, Special Issue on Hardware Security, 2014
- IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS), Special Issue on Low-Power, Reliable, and Secure Solutions for Realization of Internet of Things, 2012
- IEEE Design and Test, Special Issue on Verifying Physical Trustworthiness of Integrated Circuits and Systems, January 2010

- **General Chair**

- IEEE CANDE (Computer-Aided Network DEsign) Committee, 2012-present
- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2014
- ACM CCS CyCar (Workshop on Security, Privacy and Dependability for Cyber Vehicles), 2013

- **Organizing Committee**

- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2009-Present
- Network and Distributed System Security Symposium (NDSS), 2016-Present

- **Program Chair, Treasurer, Secretary**

- IEEE CANDE (Computer-Aided Network DEsign) Committee, 2009-2011
- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2012-13

- **Steering Committee Member, Industrial Liaison, and publicity chair**

- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2009-2011

- **IEEE/ACM Society Activities**

- ACM SIGDA Technical Committee on FPGAs and Reconfigurable Computing (TC-FPGA), 2018-Present
- IEEE Signal Processing Society (SP) member of the Information Forensics and Security Technical Committee, 2015-Present
- IEEE Circuits and Systems Society (CASS) representative for IEEE SYSC Technical Committee on Security and Privacy in Complex Information Systems, 2011-2013

- **Technical Program Committee (TPC) Memberships**

- USENIX Security Symposium, 2014-Present
- ACM/IEEE Design Automation Conference (DAC), security track chair, 2014-2016 (area chair), 2019
- Internet Society Network and Distributed System Security Symposium (NDSS), 2016-Present
- IEEE Symposium on Security and Privacy (Oakland, S&P), 2009, 2014-Present
- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2009-Present
- International Conference on Computer-Aided Design (ICCAD), (area chair), 2019
- Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2014
- ACM Conference on Computer and Communications Security (CCS), 2013
- ACM/IEEE Design Automation Conference (DAC), 2009-2011
- IEEE Conference on Computer Communications (INFOCOM), 2007, 2009-2012
- Workshop on Special Aspects of Cyber Physical Systems: Trustworthy Embedded Devices (TRUSTED), 2011
- IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2010
- IEEE Workshop on Hardware-Oriented Security and Trust (HOST), 2008-2010
- IEEE/ACM International Conference on Computer Aided Design (ICCAD), 2007
- IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), 2008
- Great Lakes Symposium on VLSI (GLVLSI), 2007-2009, 2016
- IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2007
- IEEE Statistical Signal Processing Workshop (SSP), 2007
- IEEE/ACM International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES), 2007

- **Reviewer for:**

- ACM Transactions on Reconfigurable Technology and Systems (TRETs)
- ACM Transactions on Embedded Computing Systems (TECS)
- ACM Transactions on Information and System Security (TISSEC)
- ACM Transactions on Design Automation of Electronic Systems (TODAES)

- IEEE Transactions on Computer Aided Design (TCAD)
- IEEE Transactions on Emerging Topics in Computing (TETC)
- IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Mobile Computing (TMC)
- ACM Transactions on Sensor Networks (TOSN)
- IEEE Transactions on Wireless Communications
- IEEE/ACM Transactions on Networking (TON)

- **Technical Advising**

- Expert Technical Advisor to Judge Ron Clark, United States District Court, 2009-2010

- **Invited talks:**

- Invited colloquium/seminar speaker at many academic institutions, including Boston U, Caltech, CMU, MIT, Purdue, Stanford, TU Darmstadt, UC Berkeley, UC Los Angeles, UC San Diego, U of Illinois Urbana-Champaign, U of Minnesota, U of Washington Seattle, and USC
- Invited speaker at major semiconductor design, research and development companies including IBM, TI, Qualcomm, and Intel, at several army workshops organized by DARPA, ARO, DoD, and Homeland Security, and at the National Security Agency (NSA)

- **Other:**

- Academic advisor, ARO Strategy Advisory Meeting, 2014
- Founder and faculty advisor, Women ExCEL (Electrical & Computer Engineering Leaders), 2008-Present
- Co-Founder and Co-PI, NSF Trust-Hub Community Research Initiative for Hardware Security and Trust, 2011-Present
- Panel member, NSF Directorate for Computer & Information Science (CISE), multiple times 2007, 2008, 2009, 2011, 2015
- Panel member, NSF Advance workshop for women in science and engineering, Rice University, 2006-2009