Secure, Trusted, and Assured Microelectronics (STAM) Center,
Ira A. Fulton Schools of Engineering,
Arizona State University
☎ *(602) 543-4683*
✉ *mkinsy@asu.edu*

Michel A. Kinsy

Curriculum Vitae

Technical Expertise

Computer architecture and microelectronics security, with particular emphasis on: microarchitecture security, hardware security primitives, quantum-proof cryptosystems design, self-aware polymorphous architectures, and compute acceleration engine architectures.

Education

2013 **Ph.D., Electrical Engineering and Computer Science**.
Massachusetts Institute of Technology, Cambridge, MA.
Thesis: "Many-core Architectures with Time Predictable Execution Support for Hard Real-time Applications"
Thesis advisor: Srinivas Devadas
Minor in Finance, Sloan School of Management.

2009 **M.S., Electrical Engineering and Computer Science**.
Massachusetts Institute of Technology, Cambridge, MA.
Thesis Title: "Application-Aware Deadlock-Free Oblivious Routing"
Thesis advisor: Srinivas Devadas.

2007 **B.S.E, Computer Systems Engineering**, *Arizona State University*, Tempe, AZ.
Magna Cum Laude.

2007 **B.S., Computer Science**, *Arizona State University*, Tempe, AZ.
Magna Cum Laude.

Appointments

Aug. 2021–present — Founder & Director,
Secure, Trusted, and Assured Microelectronics (STAM) Center
Ira A. Fulton Schools of Engineering, Arizona State University.
The center conducts fundamental research in technical areas meant to establish the foundation for future secure and trusted semiconductor/microelectronics technologies deployed in applications of national security importance.

Aug. 2021–present — Tenured Associate Professor,
Ira A. Fulton Schools of Engineering, Arizona State University.
Director of the Adaptive and Secure Computing Systems (ASCS) Laboratory

Aug. 2021–present — Adjunct Professor,
Department of Electrical and Computer Engineering, Texas A&M University.
Research and training efforts on microelectronics security and assurance.

2020–2021 Associate Director,
Texas A&M Cybersecurity Center, Texas A&M University.
A Board of Regents approved center at Texas A&M University that serves as the hub for cybersecurity programs across the university.

2020–2021 Tenured Associate Professor,
Department of Electrical and Computer Engineering, Texas A&M University.
Director of the Adaptive and Secure Computing Systems (ASCS) Laboratory

2016–2020 Assistant Professor,
Department of Electrical and Computer Engineering, Boston University.
Director of the Adaptive and Secure Computing Systems (ASCS) Laboratory

2014–2016 Assistant Professor,
Department of Computer and Information Science, University of Oregon.
Director of the Computer Architecture and Embedded Systems (CAES) Laboratory

2014–2016 Research Affiliate,
Computer Science and Artificial Intelligence Laboratory (CSAIL),
Massachusetts Institute of Technology.

2013–2014 Cleared Technical Staff,
Lincoln Laboratory (FFRDC)
Massachusetts Institute of Technology.
Advanced Computer Concepts: Photonically Optimized Embedded Microprocessors (POEM) to demonstrate the integration of photonics technologies within embedded microprocessors for seamless, energy-efficient, high-capacity communications.

Self-Aware Secure Architectures: Cognitive and adaptive architectures that are able to reason about the trade-off between the precision of results and the computational time and enforce execution security policies.

2010–2013 Research Assistant, Institute for Soldier Nanotechnologies, MIT.
Ivan Celanovic Group
MARTHA Project: Work in this laboratory focuses on advanced nanotechnology research to improve the survival of future soldiers. One of the mission areas is next generation high-performance computing. I led the design efforts for a prototype time-predictable computer architecture for cyber-physical systems, called MARTHA (Multicore Architecture for Real-Time Hybrid Applications).

2007–2013 Research Assistant, Computer Science and Artificial Intelligence Laboratory, MIT.
Computation Structures Group
Srinivas Devadas Group
Research Activities: Emerging computing models and technologies: reconfigurable multi-core substrate, networks-on-chip (NoCs), systems-on-chip (SoCs), embedded systems, hardware security, heterogeneous systems, and high performance computing.

Awards and Honors

Computing Research Association (CRA) Inaugural Skip Ellis Early Career Award, *The award is given annually to a person who has made significant research contributions in computer science and/or engineering and has contributed to the profession, especially in outreach to underrepresented demographics.*

IEEE International Parallel & Distributed Processing Symposium (IPDPS) Best Paper Award, *2021.*

ACM Great Lakes Symposium on VLSI (GLSVLSI) Best Paper Award, *2020.*

IEEE International Conference on Computer Design (ICCD) Best Paper Award in Test, Verification and Security Track, *2020.*

MWSCAS The Myril B. Reed Best Paper Award, *2018.*

DFT Best Student Paper Award, *2017.*

FPL Tools and Open-Source Community Service Award, *2011.*

MIT Presidential Fellowship, *2007.*

Tau Beta Pi Engineering Honor Society.

Scholarly Outputs

Publication Synopsis

- Top computer architecture conferences - International Symposium on Computer Architecture (ISCA), International Symposium on High Performance Computer Architecture (HPCA), and Parallel Architectures and Compilation Techniques (PACT);
- Top conferences in design automation - Design Automation Conference (DAC), Design, Automation and Test in Europe Conference (DATE), and International Conference on Computer-Aided Design (ICCAD);
- The premier high-performance computing conference - International Conference for High Performance Computing, Networking, Storage, and Analysis (SC);
- Top conferences in reconfigurable logic - International Symposium on Field-Programmable Gate Arrays (FPGA) and International Conference on Field Programmable Logic and Applications (FPL);
- Top conferences in hardware security - International Symposium on Hardware Oriented Security and Trust (HOST) and Asian Hardware Oriented Security and Trust Symposium (AsianHOST);
- The premier on-chip interconnect networks conference - International Symposium on Networks-on-Chip (NOCS);
- The premier real-time computing systems conference - Real-Time Systems Symposium (RTSS);
- Leading journals - Transactions on Computers (TC), Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) and Transactions on Design Automation of Electronic Systems (TODAES).

Major Publications

Book Chapters

[B1] M. Kinsy: "Post-Quantum Cryptographic Hardware Primitives", Encyclopedia of Cryptography, Security and Privacy, Springer, In Press 2021

Peer-reviewed Journals

[J14] P. Yellu, L. Buell, M. Mark, M. Kinsy, D. Xu, Q. Yu: "Security Threat Analyses and Attack Models for Approximate Computing Systems: From Hardware and Micro-Architecture Perspectives", Transactions on Design Automation of Electronic Systems (**TODAES**), In Press 2021

[J13] S. Bandara and M. A. Kinsy: "Adaptive Caches as a Defense Mechanism Against Cache Side-Channel Attacks". **Journal of Cryptographic Engineering**, Springer, 2020.

[J12] E. Taheri, M. Isakov, A. Patooghy, M. A. Kinsy: "Addressing a New Class of Reliability Threats in 3-Dimensional Network-on-Chips." In the Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), 2019 (pp. 14).

[J11] L. Bu, M. Isakov and M. A. Kinsy: "RASSS: a hijack-resistant confidential information management scheme for distributed systems,"In the Institution of Engineering and Technology (**IET**) - Computers and Digital Techniques, 2019, pp. 206-217

[J10] L. Bu, M. Karpovsky and M. A. Kinsy: "Bulwark: Securing Implantable Medical Devices Communication Channels." **Computers and Security**, Elsevier, 2018, pp. 498-511.

[J9] L. Bu, M. Karpovsky and M. A. Kinsy: "Design of Reliable Storage and Compute Systems with Lightweight Group Testing Based Non-Binary Error Correction Codes." In the Institution of Engineering and Technology (**IET**) - Computers and Digital Techniques, 2018, pp. 140-153.

[J8] T. Yang, Y. Wei, Z. Tu, H. Zeng, M. Kinsy, N. Zheng and P. Ren: "Design Space Exploration of Neural Network Activation Function Circuits." In the Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), 2018, pp. 1974-1978.

[J7] L. Bu, J. Dofe, Q. Yu and M. Kinsy: "SRASA: A Generalized Theoretical Framework for Security and Reliability Analysis in Computing Systems." Journal of Hardware and Systems Security (**HaSS**) - Special Issue on Hardware Solutions for Cyber Security, 2018, pp. 200-218.

[J6] S. M. Sebt, A. Patooghy, H. Beitollahi and M. Kinsy: "Circuit Enclaves Susceptible to Hardware Trojans Insertion at Gate-Level Designs." In the Institution of Engineering and Technology (**IET**) - Computers and Digital Techniques, 2018, pp. 251-257.

[J5] L. Bu, M. Isakov and M. Kinsy: "A Secure and Robust Scheme for Sharing Confidential Information in IoT Systems." In the Elsevier Journal of **Ad Hoc Networks**, 2018, (pp. 12).

[J4] M. Kinsy, L. Bu, M. Isakov, M. Mark: "Designing Secure Heterogeneous Multicore Systems from Untrusted Components." In **Cryptography**, June 2018 (pp. 12).

[J3] P. Ren, M. Kinsy, and N. Zheng: "Fault-Aware Load-Balancing Routing for 2D-Mesh and Torus On-Chip Network Topologies." In the Transactions on Computers (**TC**), March 2016, pp. 873-887.

[J2] P. Ren, X. Ren, S. Sane, M. Kinsy, and N. Zheng: "Deadlock-Free and Connectivity-Guaranteed Methodology for Achieving Fault-tolerance in On-chip Networks." In the Transactions on Computers (**TC**), February 2016, pp. 353-366.

[J1] M. Kinsy, M. H. Cho, T. Wen, M. Lis , G. E. Suh, M. Dijk, and S. Devadas: "Optimal and Heuristic Application-Aware Oblivious Routing." In the Transactions on Computers (**TC**), January 2013, pp. 59-73.

Peer-Reviewed Conferences

[C55] M. Isakov and M. Kinsy: "SparseFabric: Ideal Topologies for Training Sparse Networks". In the The 40th IEEE International Conference on Computer Design (**ICCD**), 2022.

[C54] J. Abraham, A. Ehret, and M. Kinsy: "A Compiler for Transparent Namespace-Based Access Control for the Zeno Architecture". In the 2022 IEEE International Symposium on Secure and Private Execution Environment Design (**SEED**), 2022.

[C53] M. Isakov, M. Currier, E. del Rosario, S. Madireddy, P. Balaprakash, P. H. Carns, R. Ross, G. K. Lockwood, and M. A. Kinsy: "A Taxonomy of Error Sources in HPC I/O Machine Learning Models", In the International Conference for High Performance Computing, Networking, Storage, and Analysis (**SC**), 2022.

[C52] M. Isakov, E. Stapf, M. Mark, G. dessouky, P. Mahmoody, S. Zeitouni, A. sadeghi and M. A. Kinsy: "Distributed Memory Guard: Enabling Secure Enclave Computing in NoC-based Architectures", In the 58th ACM/EDAC/IEEE Design Automation Conference (**DAC**), 2021.

[C51] X. Wang, B. Williams, J. D. Leidel, A. Ehret, M. A. Kinsy and Y. Chen: "xBGAS: A Global Address Space Extension on RISC-V for High Performance Computing", In the 35th IEEE International Parallel & Distributed Processing Symposium (**IPDPS**), 2021. Best Paper Nominee

[C50] M. Isakov, E. del Rosario, S. Madireddy, P. Balaprakash, P. H. Carns, R. Ross, and M. A. Kinsy: "HPC I/O Throughput Bottleneck Analysis with Explainable Local Models", In the International Conference for High Performance Computing, Networking, Storage, and Analysis (**SC**), 2020.

[C49] R. Agrawal, L. Bu, and M. A. Kinsy: "Quantum-Proof Lightweight McEliece Cryptosystem Co-processor Design". In the 38th IEEE International Conference on Computer Design (**ICCD**), 2020. Best Paper in the Test, Verification and Security Tack

[C48] A. Ehret, K. M. Gettings, B. R. Jordan Jr. and M. A. Kinsy: "A Hardware Root-of-Trust Design for Low-Power SoC Edge Devices". In the 2020 IEEE High Performance Extreme Computing Conference (**HPEC**), 2020. Outstanding Student Paper Award

[C47] V. Gadepally, M. Isakov, R. Agrawal, K. Gettings, and M. Kinsy: "Homomorphic Encryption Based Secure Sensor Data Processing". In the 2020 IEEE High Performance Extreme Computing Conference (**HPEC**), 2020.

[C46] X. Wang, B. Williams, J. D. Leidel, A. Ehret, M. A. Kinsy and Y. Chen: "Remote Atomic Extension (RAE) for Scalable High Performance Computing", In the 57th ACM/EDAC/IEEE Design Automation Conference (**DAC**), 2020, pp. 1-6.

[C45] R. Agrawal, L. Bu, and M. A. Kinsy: "A Post-Quantum Secure Discrete Gaussian Noise Sampler", In IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**), 2020 pp. 1-10.

[C44] R. Agrawal, L. Bu, E. del Rosario, and M. A. Kinsy: "Towards Programmable All-Digital True Random Number Generators", In the 30th edition of the ACM Great Lakes Symposium on VLSI (**GLSVLSI**), 2020 pp. 1-6. Best Paper Award

[C43] R. Agrawal, L. Bu, E. del Rosario, and M. A. Kinsy: "Design-flow Methodology for Secure Group Anonymous Authentication." In IEEE International Conference on Design, Automation and Test in Europe (**DATE**), 2020, pp. 1-6.

[C42] P. Jamieson, M. Herbordt, and M. Kinsy: "A case study: Undergraduate self-learning in HPC including OpenMP, MPI, OpenCL, and FPGAs", In the International Conference on Computational Science and Computational Intelligence (**CSCI**), December 2019, pp. 782-787.

[C41] M. Isakov, V. Gadepally, K. M. Gettings, and M. A. Kinsy: "A Survey of Attacks and Defenses of Edge-Deployed Neural Networks." In IEEE High Performance Extreme Computing Conference (**HPEC'19**), September 2019, pp. 1-8. Best Student Paper Nominee

[C40] A. Ehret, K. M. Gettings, B. R. Jordan Jr., M A. Kinsy: "A Survey on Hardware Security Techniques Targeting Low-Power SoC Designs." In IEEE High Performance Extreme Computing Conference (**HPEC'19**), September 2019, pp. 1-8.

[C39] M. Kinsy and N. Boskov: "Secure Computing Systems Design Through Formal Micro-Contracts." In the 29th edition of the ACM Great Lakes Symposium on VLSI (**GLSVLSI**), May 2019, pp. 537-542.

[C38] P. Yellu, N. Boskov, M. A. Kinsy and Q. Yu: "Security Threats in Approximate Computing Systems." In the 29th edition of the ACM Great Lakes Symposium on VLSI (**GLSVLSI**), May 2019, pp. 387-392.

[C37] A. Ehret, M. Isakov, and M. A. Kinsy: "Towards a Generalized Reconfigurable Agent Based Architecture: Stock Market Simulation Acceleration." In the 2018 International Conference on Reconfigurable Computing and FPGAs (**ReConFig**), December 2018, pp. 1-6.

[C36] M. Isakov, L. Bu, H. Cheng, and M. A. Kinsy: "Preventing Neural Network Model Exfiltration in Machine Learning Hardware Accelerators." In the 2018 Asian Hardware Oriented Security and Trust Symposium (**AsianHOST**), December 2018, pp. 62-67.

[C35] M. Isakov and M. A. Kinsy: "NoSync: Particle Swarm Inspired Distributed DNN Training." The 27th International Conference on Artificial Neural Networks (**ICANN'18**), October 2018, pp. 607-618.

[C34] L. Bu, H. Cheng, and M. A. Kinsy: "Fast Dynamic Device Authentication Based on Lorenz Chaotic Systems." 2018 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (**DFT**), October 2018, pp. 1-6.

[C33] M. Isakov, A. Ehret, M. A. Kinsy: "Chameleon: A Generalized Reconfigurable Open-Source Architecture for Deep Neural Network Training." 2018 IEEE High Performance Extreme Computing Conference (**HPEC'18**), September 2018, pp. 1-7. Best Student Paper Nominee

[C32] H. Cheng, L. Bu, and M. Kinsy: "Adaptive and Dynamic Device Authentication Based on Lorenz Chaotic Systems." In the 61st International Midwest Symposium on Circuits and Systems (**MWSCAS**), August 2018, pp. 976-979.

[C31] L. Bu and M. A. Kinsy: "Weighted Group Decision Making Using Multi-identity Physical Unclonable Functions." International Conference on Field-Programmable Logic and Applications (**FPL2018**), August 2018, pp. 251-254.

[C30] M. Isakov, A. Ehret and M. A. Kinsy: "ClosNets: Batchless DNN Training with On-Chip A Priori Sparse Neural Topologies." International Conference on Field-Programmable Logic and Applications (**FPL2018**), August 2018, pp. 55-59.

[C29] L. Bu, M. Mark and M. A. Kinsy: "A Short Survey at the Intersection of Reliability and Security in Processor Architecture Designs." IEEE Computer Society Annual Symposium on VLSI (**ISVLSI'18**), July 2018, pp. 118-123.

[C28] S. Kashi, A. Patooghy, D. Rahmati, M. Fazeli and M. A. Kinsy: "Application Specific Networks-on-Chip Synthesis: An Energy Efficient Approach." IEEE Computer Society Annual Symposium on VLSI (**ISVLSI'18**), July 2018, pp. 52-57.

[C27] E. Aerabi, A. Patooghy, H. Rezaei, M. Mark, M. Fazeli and M. Kinsy: "Mystic: Mystifying IP Cores Using an Always-ON FSM Obfuscation Method." IEEE Computer Society Annual Symposium on VLSI (**ISVLSI'18**), July 2018, pp. 626-631.

[C26] A. Ehret, P. Jamieson and M. A. Kinsy: "Scalable Open-Source Reconfigurable Architecture for Bacterial Quorum Sensing Simulations." International Symposium on Highly Efficient Accelerators and Reconfigurable Technologies (**HEART'18**), June 2018, pp. 1-5.

[C25] Bu and M. Kinsy: "Hardening AES Hardware Implementations Against Fault and Error Inject Attacks." In the 28th edition of the ACM Great Lakes Symposium on VLSI (**GLSVLSI**), May 2018, pp. 499-502.

[C24] K. Soleimani, A. Patooghy, N. Soltani, L. Bu, M. A. Kinsy: "Crosstalk Free Coding Systems to Protect NoC Channels Against Crosstalk Faults." In 2017 IEEE 35th International Conference on Computer Design (**ICCD**), November 2017, pp. 385-390.

[C23] J. R. Doppa, R. G. Kim, M. Isakov, M. A. Kinsy, H. Kwon and T. Krishna: "Adaptive Manycore Architectures for Big Data Computing." In the International Symposium on Networks-on-Chip (**NOCS**), October 2017, pp. 1-8.

[C22] L. Bu, H. D. Nguyen, and M. A. Kinsy: "RASSS: A perfidy-aware protocol for designing trustworthy distributed systems." In the 2017 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (**DFT**), October 2017, pp. 1-6. Best Student Paper Award and Best Paper Nominee

[C21] E. Taheri, M. Isakov, A. Patooghy, and M. Kinsy: "Advertiser Elevator: a Fault Tolerant Routing Algorithm for Partially Connected 3D Network-on-Chips." In the 60th International Midwest Symposium on Circuits and Systems (**MWSCAS**) August 2017, pp. 136-139.

[C20] H. Hosseinzadeh, M. Isakov, M. Darabi, A. Patooghy, and M. Kinsy: "Janus: An uncertain cache architecture to cope with side channel attacks." In the 60th International Midwest Symposium on Circuits and Systems (**MWSCAS**) August 2017, pp. 827-830. The Myril B. Reed Best Paper Award

[C19] M. Kinsy, S. Khadka and M. Isakov: "PreNoc: Neural Network based Predictive Routing for Network-on-Chip Architectures." In the 27th edition of the ACM Great Lakes Symposium on VLSI (**GLSVLSI**), May 2017, pp. 65-70.

[C18] M. Kinsy, S. Khadka, M. Isakov and A. Farrukh: "Hermes: Secure Heterogeneous Multicore Architecture Design." In the IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**), May 2017, pp. 14-20

[C17] P. Ren, M. Kinsy, M. Zhu and N. Zheng: "Towards Connectivity-Guaranteed Power-gating Large-scale On-chip Networks", The 7th International Green and Sustainable computing conference (**IGSC**), Nov 7-9, 2016, pp. 1-6.

[C16] J. Mohr and M. Kinsy: "Securitas: Multi-Tenant Secure Computer Architecture." In the 40th Government Microcircuit Applications and Critical Technology Conference (**GOMACTech-15**), April 2015, (pp. 6).

[C15] M. Kinsy and S. Devadas: "Low-Overhead Hard Real-time Aware Interconnect Network Router." In IEEE High Performance Extreme Computing (**HPEC**), September, 2014, pp. 1-6.

[C14] M. Kinsy and S. Devadas: "Algorithms for Scheduling Task-based Applications onto Heterogeneous Many-core Architectures." In IEEE High Performance Extreme Computing (**HPEC**), September 2014, pp. 1-6.

[C13] M. Kinsy, I. Celanovic, O. Khan, and S. Devadas: "MARTHA: Architecture for Control and Emulation of Power Electronics and Smart Grid Systems." In IEEE International Conference on Design, Automation and Test in Europe (**DATE**), March 2013, pp. 519-524.

[C12] M. Kinsy, M. Pellauer, and S. Devadas: "Heracles: A Tool for Fast RTL-Based Design Space Exploration of Multicore Processors." In Proceedings of the 21st International Symposium on Field-Programmable Gate Arrays (**FPGA**), February 2013, pp. 125-134.

[C11] J. Poon, M. Kinsy, N. Pallo, S. Devadas, and I. Celanovic: "Hardware-in-the-loop testing for electric vehicle drive applications." In Proceedings of the 27th Annual IEEE Applied Power Electronics Conference and Exposition (**APEC**), February 2012, pp. 2576-2582.

[C10] M. Kinsy, O. Khan, I. Celanovic, M. Dusan, N. Celanovic, and S. Devadas: "Time-Predictable Computer Architecture for Cyber-Physical Systems: Digital Emulation of Power Electronics Systems." In Proceedings of the 32nd Real-Time Systems Symposium (**RTSS**), December 2011, pp. 305-316.

[C9] M. Kinsy, M. Pellauer, and S. Devadas: "*Heracles*: Fully Synthesizable Parameterized MIPS-Based Multicore System." In Proceedings of the 21st International Conference on Field Programmable Logic and Applications (**FPL**), September 2011, pp. 356-362. Tools and Open-Source Community Service Award

[C8] M. Lis, K. S. Shim, M. H. Cho, C. Fletcher, M. Kinsy, I. Lebedev, O. Khan, and S. Devadas: "Brief Announcement: Distributed Shared Memory based on Computation Migration." In Proceedings of the 23rd Symposium on Parallelism in Algorithms and Architectures (**SPAA**), June 2011, pp. 253-256.

[C7] M. Kinsy, D. Majstorovic, P. Haessig, J. Poon, N. Celanovic, I. Celanovic, and S. Devadas: "High-Speed Real-Time Digital Emulation for Hardware-in-the-Loop Testing of Power Electronics: A New Paradigm in the Field of Electronic Design Automation (EDA) for Power Electronics Systems." In Proceedings of the 2011 International Exhibition & Conference for Power Electronics, Intelligent Motion, Power Quality (**PCIM Europe**), May 2011 (pp. 6).

[C6] M. Pellauer, M. Adler, M. Kinsy, A. Parashar, and J. Emer: "HAsim: FPGA-based high-detail multicore simulation using time-division multiplexing." In Proceedings of the 17th International Symposium on High Performance Computer Architecture (**HPCA**), February 2011, pp. 406-417.

[C5] M. H. Cho, M. Lis, K. S. Shim, M. Kinsy, T. Wen, and S. Devadas: "Oblivious Routing in On-Chip Bandwidth-Adaptive Networks." In Proceedings of the Parallel Architectures and Compilation Techniques (**PACT**), September 2009, pp. 181-190.

[C4] M. Kinsy, M. H. Cho, T. Wen, G. E. Suh, M. Dijk, and S. Devadas: "Application-Aware Deadlock-Free Oblivious Routing." In Proceedings of the International Symposium on Computer Architecture (**ISCA**), June 2009.

[C3] K. S. Shim, M. H. Cho, M. Kinsy, T. Wen, M. Lis , G. E. Suh, and S. Devadas: "Static Virtual Channel Allocation in Oblivious Routing." In Proceedings of the International Symposium on Networks-on-Chip (**NOCS**), May 2009, pp. 38-43.

[C2] M. H. Cho, C-C. Cheng, M. Kinsy, G. E. Suh, and S. Devadas: "Diastolic Arrays: Throughput-Driven Reconfigurable Computing." In Proceedings of the International Conference on Computer-Aided Design (**ICCAD**), November 2008, pp. 457-464.

[C1] M. Kinsy and Z. Lacroix: "Storing Efficiently Bioinformatics Workflows." In Proceedings of the 2007 IEEE International Symposium on Bioinformatics Bioengineering (**BIBE**), October 2007, pp. 1328-1332.

Peer-Reviewed Workshops

[W16] E. del Rosario, M. Currier, Mihailo Isakov, S. Madireddy, P. Balaprakash, P. H. Carns, R. Ross, K. Harms, S. Snyder, and M. A. Kinsy: "Gauge: An Interactive Data-Driven Visualization Tool for HPC Application I/O Performance Analysis", In the 5th International Parallel Data Systems Workshop (**PDSW 2020**) at SC20.

[W15] M. Isakov, E. del Rosario, S. Madireddy, P. Balaprakash, P. H. Carns, R. Ross, and M. A. Kinsy: "Towards Generalizable Models of I/O Throughput", In the 10th International Workshop on Runtime and Operating Systems for Supercomputers (**ROSS 2020**) at SC20.

[W14] S. Bandara and M. A. Kinsy:"Adaptive Caches as a Defense Mechanism Against Cache Side-Channel Attacks". In 3rd Attacks and Solutions in Hardware Security Workshop (**ASHES**), 2019.

[W13] R. Agrawal, S. Bandara, A. Ehret, M. Isakov, M. Mark, and M. A. Kinsy: "The BRISC-V Platform: A Practical Teaching Approach for Computer Architecture". In Workshop on Computer Architecture Education in conjunction with ISCA (**WCAE**), 2019.

[W12] L. Bu, R. Agrawal, H. Cheng and M. A. Kinsy: "A Lightweight McEliece Cryptosystem Co-Processor Design". Boston Area Architecture 2019 Workshop (**BARC19**), 2019.

[W11] N. Boskov, M. Isakov and M. A. Kinsy: "CodeTrolley: Hardware-Assisted Control Flow Obfuscation". Boston Area Architecture 2019 Workshop (**BARC19**), 2019.

[W10] M. Graziano, M. Mark, S. Gvozdenovic and M. A. Kinsy: "Hardware Assisted Transparent ROP Mitigation for RISC-V". Boston Area Architecture 2019 Workshop (**BARC19**), 2019.

[W9] L. Bu, R. Agrawal, H. Cheng and M. A. Kinsy: "Post-Quantum Cryptographic Hardware Primitives". Boston Area Architecture 2019 Workshop (**BARC19**), 2019.

[W8] S. Bandara, A. Ehret, D. Kava and M. A. Kinsy: "BRISC-V: An Open-Source Architecture Design Space Exploration Toolbox",27th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (**FPGA**), 2019.

[W7] M. A. Kinsy, D. Kava, A. Ehret and M. Mark: "Sphinx: A Secure Architecture Based on Binary Code Diversification and Execution Obfuscation." Boston Area Architecture 2018 Workshop (**BARC18**), January 2018.

[W6] M. A. Kinsy, M. Isakov, A. Ehret and D. Kava: "SAPA: Self-Aware Polymorphic Architecture." Boston Area Architecture 2018 Workshop (**BARC18**), January 2018.

[W5] M. Isakov and M. A. Kinsy: "ClosNets: a Priori Sparse Topologies for Faster DNN Training." Boston Area Architecture 2018 Workshop (**BARC18**), January 2018.

[W4] M. Kinsy, R. Agrawal and H. Nguyen: "Fast Processing of Large Graph Applications Using Asynchronous Architecture." Boston Area Architecture 2017 Workshop (**BARC17**), January 2017.

[W4] M. Kinsy and S. Devadas: "Heracles 2.0: A Tool for Design Space Exploration of Multi/Many-core Processors." Workshop on the Intersections of Computer Architecture and Reconfigurable Logic (**CARL** 2012) Co-located with ISCA-39, June 2012.

[W3] M. H. Cho, M. Lis, K. S. Shim, M. Kinsy, and S. Devadas: "Path-Based, Randomized, Oblivious Routing." In Proceedings of the 2nd International Workshop on Network-on-Chip Architectures (**NoCArc'09**), December 2009.

[W2] Q. Shao, M. Kinsy and Y. Chen: "Storing and Discovering Critical Workflows from Log in Scientific Exploration." In Proceedings of the 2007 IEEE International Workshop on Scientific Workflows (**SWF**), July 2007.

[W1] M. Kinsy, Z. Lacroix, C. Legendre, P. Wlodarczyk, N. Yacoubi Ayadi: "ProtocolDB: Storing Scientific Protocols with a Domain Ontology." Lecture Notes in Computer Science by Springer-Verlag. **WISE** Workshops 2007: 17-28

Peer-reviewed Posters

[P8] X. Wang, J. D. Leidel, B. Williams, A. Ehret, M. Mark, M. Kinsy, and Y. Chen: "xBGAS: An Address Space Extension for Scalable High-Performance Computing", In the International Conference for High Performance Computing, Networking, Storage, and Analysis (**SC**), 2020.

[P7] R. Agrawal, L. Bu, and M. A. Kinsy: "Fast Arithmetic Hardware Library For RLWE-Based Homomorphic Encryption." In the 28th IEEE International Symposium On Field-Programmable Custom Computing Machines (**FCCM**), 2020

[P6] M. Mark, D. Whelihan, M. Vai, H. Whitman, M A. Kinsy: "Resilience-Aware Decomposition and Monitoring of Large-Scale Embedded Systems." In IEEE High Performance Extreme Computing Conference (**HPEC'19**), 2019

[P5] M. Isakov and M. A. Kinsy: "NeuroFabric: A Priori Sparsity for Training on the Edge?. In the 2019 tinyML Summit (**tinyML**), 2019.

[P4] R. S. Agrawal and M. A. Kinsy: "Adaptive-Approximate Cache Architecture." In the 3rd Career Workshop for Women and Minorities in Computer Architecture, held in conjunction with the 50th IEEE/ACM International Symposium on Microarchitecture **MICRO-50**), October 2017.

[P3] S. Khadka, S. Ergullu-Koehnen, B. Gravelle, and M. Kinsy: "Neural network based predictive routing for network-on-chip architectures." Work-in-Progress Presentation at 53rd Design Automation Conference (**DAC** 2016), June 2016.

[P2] P. Ren, M. Kinsy, C. Yang, B. Gravelle, S. Khadka, and N. Zheng: "Copal: Connectivity preserving algorithm for network-on-chip power-gating." Work-in-Progress Presentation at 53rd Design Automation Conference (**DAC** 2016), June 2016.

[P1] M. Kinsy, J. Poon, I. Celanovic, O. Khan, and S. Devadas: "A Multicore Architecture for Control and Emulation of Power Electronics and Smart Grid Systems Under Hard Real-Time Constraints." Work-in-Progress Presentation at 49th Design Automation Conference (**DAC** 2012), June 2012.

Reports

[R4] A. Ehret, J. Abraham, M. Isakov, M. A. Kinsy. "Zeno: A scalable capability-based secure architecture." arXiv preprint arXiv:2208.09800, 2022.

[R3] M. Isakov and M. A. Kinsy. "Drndalo: Lightweight Control Flow Obfuscation Through Minimal Processor/Compiler Co-Design." arXiv arXiv:2002.08339, 2020.

[R3] N. Boskov, M. Isakov, M. A. Kinsy. "NeuroFabric: Identifying Ideal Topologies for Training A Priori Sparse Networks." arXiv arXiv:1912.01560, 2019.

[R2] P. Ren, M. Kinsy, M. Zhu, S. Khadka, M. Isakov, A. Ramrakhyani, T. Krishna, and N. Zheng. "FASHION: Fault-Aware Self-Healing Intelligent On-chip Network." arXiv preprint arXiv:1702.02313, 2017.

[R1] M. Kinsy and R. Uhler: "SHA-3: FPGA implementation of ESSENCE and ECHO hash algorithm candidates using Bluespec." CSG-Report, CSAIL, MIT, May, 2009

Students Mentoring

Graduated Advisees

Ph.D. 2022	Alan Ehret, Computer Engineering, Arizona State University Thesis Title: Eleatic: Secure Architecture Across the Edge-to-Cloud Continuum
Ph.D. 2022	Mihailo Isakov, Computer Engineering, Arizona State University Thesis Title: Self-Aware Adaptive General-Purpose Computing Architectures
Ph.D. 2019	Lake Bu, Electrical and Computer Engineering, Boston University - Draper Laboratory Thesis Title: Design of Secure and Trustworthy System-on-Chip Architectures using Hardware-based Root-of-Trust Techniques
M.S. 2022	Jacob Abraham, Computer Engineering, Arizona State University - HP Enterprise - Thesis Title: Code Generation Techniques for Emerging Capability Architectures
M.S. 2021	Miguel Mark, Electrical and Computer Engineering, Texas A&M University
M.S. 2019	Sahan Bandara, Electrical and Computer Engineering, Boston University - BU ECE Ph.D. Program - Thesis Title: Investigating the Viability of Adaptive Caches as a Defense Mechanism Against Cache Side-Channel Attacks
M.S. 2019	Donato Kava, Electrical and Computer Engineering, Boston University - (First Employment) MIT Lincoln Laboratory
M.S. 2018	Shreeya Khadka, Electrical and Computer Engineering, Boston University - NVIDIA Corporation
M.S. 2018	Hien Nguyen, Electrical and Computer Engineering, Boston University - JDA Software
M.S. 2017	Rashmi Agrawal, Electrical and Computer Engineering, Boston University. M.S. Project: Adaptive-Approximate Cache Architecture - Intel Corporation
M.S. 2016	Joseph Mohr, Computer and Information Science, University of Oregon. M.S. Project: Securitas: Multi-Tenant Secure Computer Architecture - University of Oregon
B.S. 2016-20	Emma Howard, Karanraj Chauhan, Byoungsul Lee, Boston University
B.S 2017	Haley Whitman, University of Oregon - MIT Lincoln Laboratory
B.S. 2015-17	Andrew Hill, Jack Ziesing, University of Oregon

Research Mentoring Activities

2019-2020	Eliakin Del Rosario, Research Assistant
2018-19	Dr. Hai Cheng, Visiting Research Fellow
2017-2018	Dr. Ahmad Patooghy, Postdoctoral Fellow - Assistant Professor at the University of Central Arkansas
2017-2018	Miguel Mark, Research Assistant
2015-2016	Dr. Christopher Dudley, Research Fellow
2014-2016	Jacob Riddle, Research Assistant
2014-2015	Sena Ergullu Koehnen, Research Assistant
2015-2016	Piotr Esden-Tempski, Research Assistant

Institutional Research Support

Defended October 2022	Quoc Long Vinh Ta, M.S. Thesis Committee, School of Computing and Augmented Intelligence, Arizona State University
Defended August 2019	Chen Yang, Ph. D. Dissertation Committee, Dept. of Electrical and Computer Engineering, Boston University
Defended July 2019	Onur Sahin, Ph. D. Dissertation Committee, Dept. of Electrical and Computer Engineering, Boston University
Defended August 2017	Jiayi Sheng, Ph. D. Dissertation Committee, Dept. of Electrical and Computer Engineering, Boston University
Defended August 2017	Ryan Silva, Ph. D. Dissertation Committee, Dept. of Electrical and Computer Engineering, Boston University
Defended April 2017	Zafar Takhirov, Ph. D. Dissertation Committee, Dept. of Electrical and Computer Engineering, Boston University
Defended December 2016	Tiansheng Zhang, Ph. D. Dissertation Committee, Dept. of Electrical and Computer Engineering, Boston University
Defended September 2017	Anmol Gupta, M.S. Thesis Committee, Dept. of Electrical and Computer Engineering, Boston University
2016	Chad Wood, Directed Research Project Committee Member, Dept. of Computer and Information Science, University of Oregon
2016	Sabin Kafle, Directed Research Project Committee Member, Dept. of Computer and Information Science, University of Oregon
2015	Robert Lim, Directed Research Project Committee Member, Dept. of Computer and Information Science, University of Oregon
2015	Kanika Sood, Directed Research Project Committee Member, Dept. of Computer and Information Science, University of Oregon
2014-2016	Hao Wang, Dissertation Advisory Committee Member, Dept. of Computer and Information Science, University of Oregon
2014-2015	Amir Farzad, Dissertation Advisory Committee Member, Dept. of Computer and Information Science, University of Oregon
Defended May 2016	Bryson Nakamura, Ph. D. Dissertation Committee, Dept. of Human Physiology, University of Oregon
2015-2016	Brittany White, Ph. D. Dissertation Committee, Dept. of Biochemistry and Chemistry, University of Oregon

Teaching Experience

Essential Course Development

Graduate Level Courses

Fall 2022 **CSE/CEN 598: Hardware Security & Trust**, *Arizona State University, Ira A. Fulton Schools of Engineering*.

This course provides an in-depth introduction to the role of hardware security and trust in computing systems. Topics covered are : integrity and authentication, encryption algorithms, key distribution and management, hardware Trojans, side-channel attacks, hardware counterfeiting, circuit obfuscation, trust platform modules, physical unclonable functions, true random number generators, homomorphic encryption, multi-party computation, trusted execution environments, etc. `https://ascslab.org/courses/CSECEN598/index.html`.

Spring 2021 **ECEN 676: Advanced Computer Architecture**, *Texas A&M University, College of Engineering*.

Topics covered advanced topics in instruction set design, pipelined, out-of-order and speculative executions, superscalar, very long instruction word (VLIW), vector, and multithreaded processors, cache and virtual memory organizations, synchronization, memory models, and cache coherence protocols for multiprocessors, multithreaded architectures, multiprocessor interconnection networks.

Spring 2020, Fall 2018 **EC 700/500: Hardware and Systems Security**, *Boston University, College of Engineering*.

In-depth inspection of the role that hardware security plays in cybersecurity and computer hardware related attacks and defense in computing systems. The topics covered are: classic and Modern encryption algorithms, integrity and authentication, key distribution and management, hardware Trojans, side-channel attacks, fault attacks, hardware counterfeiting, oblivious RAM, digital signatures, circuit obfuscation, trust platform modules, physical unclonable functions, true random number generators, and secure architecture designs.The class project consists of building secure multi-core RISC-V ISA architecture.

Spring 2018 **EC 513: Computer Architecture**, *Boston University, College of Engineering*.

Examination of the evolution and the principles underlying modern computer architectures. It emphasizes the fundamental relationship between technology, hardware organization, and programming systems. Topics covered include processor micro-architecture, instruction set design, pipelined, out-of-order, and speculative execution, superscalar, very long instruction word (VLIW), vector, and multithreaded processors, cache and virtual memory organizations, synchronization, memory models, and cache coherence protocols for multiprocessors, multithreaded architectures, multiprocessor interconnection networks, and embedded systems.

Winter 2016 | Fall 2014 **CIS 429/529: Computer Architecture**, *University of Oregon, Dept. of Computer and Information Science*.

The objectives are to provide students a strong understanding of modern computing systems.

Spring 2015 | Spring 2016 **CIS 407/507: Complex Digital System Design**, *University of Oregon, Dept. of Computer and Information Science*.

The course introduces architecture and design concepts underlying modern complex VLSIs and system-on-chips. The class has senior undergraduate and graduate students from the Computer and Information Science and Physics departments.

IAP 2012 **6.S918: Design and Exploration of Multicore Systems with Heracles - Instructor**, *Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science*.

The goal in the class is to perform multi-core and many-core architectures design space exploration using the Heracles Multicore System infrastructure. We examine different implementation choices: core micro-architecture, levels of caches, cache sizes, routing algorithm, router micro-architecture, distributed or shared memory, or network interface, and evaluate their impact on the overall system performance. `http://stellar.mit.edu/S/course/6/ia12/6.S918/`.

Undergraduate Level Courses

Spring 2022 **CSE 420: Computer Architecture I**, *Arizona State University, Ira A. Fulton Schools of Engineering*.

The course will introduction students to the evolution and the principles underlying modern computer architectures. It will emphasize the fundamental relationship between technology, hardware organization, and programming systems. Topics covered in the class will include processor micro-architecture, instruction set design, pipelined, out-of-order, and speculative execution, superscalar, very long instruction word (VLIW), vector, and multithreaded processors, cache and virtual memory organizations, synchronization, memory models, and cache coherence protocols for multiprocessors, multithreaded architectures, and multiprocessor interconnection networks. `https://ascslab.org/courses/CSE420/index.html`.

Fall 2017 | Spring 2019 | Fall 2019 **EC 413: Computer Organization**, *Boston University, College of Engineering*.

Introduction to the fundamentals and design of computer systems. Topics covered include computer instruction sets, assembly language programming, arithmetic circuits, CPU design (data path and control, pipelining), performance evaluation, memory devices, memory systems including caching and virtual memory, and I/O. A single-cycle RISC processor design project using design automation tools.

Fall 2017 **EK100: Freshmen Seminar**, *Boston University, College of Engineering*.

First-year experience course that introduces students to Boston University, the College of Engineering, and the field of engineering.

Fall 2016 **EK131/132: Introduction to Engineering**, *Boston University, College of Engineering*.

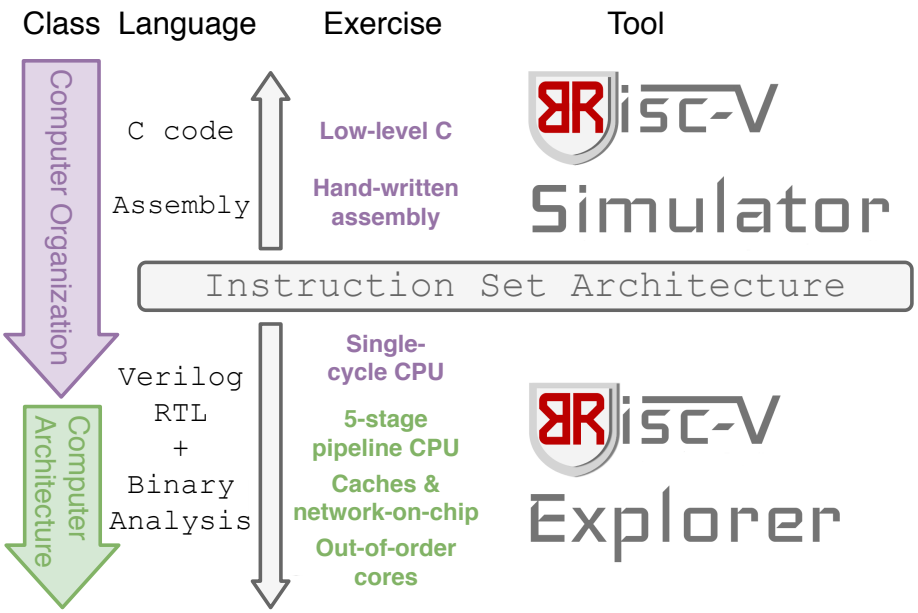
The class introduces students to engineering analysis and design. Topics covered in the class include: introduction to analog and digital systems, binary number system, electronic components, RC circuit, circuit analysis, combinational and sequential circuits, micro-control design, and system programming.

Fall 2015 **CIS 314: Computer Organization**, *University of Oregon, Dept. of Computer and Information Science*.

This course covers the basics of computer organization with emphasis on register-level computer organization, instruction set architecture, and assembly language programming.

Development & Publication of Instructional Materials

Instructional Materials to Improve Computer Organization/Architecture Teaching: My team and I have designed and released two of the most used RISC-V based tools for teaching both computer organization and architecture courses nationally - i.e., BRISCV/Trireme Simulator and Emulator [1,2]. [Link]



[1] R. Agrawal, S. Bandara, A. Ehret, M. Isakov, M. Mark, and M. A. Kinsy: *The BRISC-V Platform: A Practical Teaching Approach for Computer Architecture*, In Workshop on Computer Architecture Education (WCAE) - Co-located with the International Symposium on Computer Architecture (ISCA), 2019.

[2] P. Jamieson, M. Herbordt and M. Kinsy: *A Case Study: Undergraduate Self-Learning in HPC Including OpenMP, MPI, OpenCL, and FPGAs*, 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2019, pp. 782-787.

Instructional Materials to Improve Secure Systems Teaching: My team and I have designed and

College Teaching Support

Fall 2017 **EC 444 Smart and Connected Systems**, *Boston University, College of Engineering*.
Led the efforts in the conception of the course with Profs. David Starobinski and Thomas Little, under the college's Future of Undergraduate Engineering Education Task Force.

Invited Significant Seminars

Recent Invited Talks

Host Dr. Rosario Cammarota — *HERISCV: Homomorphic-Encryption Enabled RISC-V Candidate Architecture*, Intel Labs, 2022.

Host Prof. Wayne Burleson — *Establishing the Essential Hardware Primitives for Quantum-Proof Secure Computer Systems*, ECE Department, College of Engineering, University of Massachusetts Amherst, 2020.

Host Prof. Margaret Martonosi — *Establishing the Essential Hardware Primitives for Quantum-Proof Secure Computer Systems*, Department of Computer Science, Princeton University, 2019.

Host Prof. Mieszko Lis — *Hardware Primitives for Quantum-Proof Secure Computer Systems*, Department of Electrical and Computer Engineering, University of British Columbia, 2019.

Host Prof. Natalie Enright Jerger	*Neural Network Model Exfiltrations in Edge Devices*, Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, 2019.
Host Prof. Yan Solihin	*Towards Secure Execution of Neural Network Models on Edge Devices*, Department of Computer Science, University of Central Florida, 2019.
DASS'19	*Preventing Neural Network Model Exfiltration in Machine Learning Hardware Accelerators*, at SIGDA Design Automation Summer School (DASS) - ACM/IEEE Design Automation Conference (DAC), 2019.
Host Prof. Wayne Burleson	*Trusted Inference Engine: Preventing Neural Network Model Exfiltration in Edge Devices*, ECE Department, College of Engineering, University of Massachusetts Amherst, 2019.
Host Prof. Farinaz Koushanfar	*Preventing Neural Network Model Exfiltration in Machine Learning Hardware Accelerators*, ECE Department, Jacobs School of Engineering, University of California, San Diego, 2018.
Host Prof. Xuehai Qian	*Trusted Inference Engine: Preventing Neural Network Exfiltration in Hardware Devices*, Ming Hsieh Department of Electrical and Computer Engineering, University of Southern California, 2018.
Host Prof. Russell Joseph	*Trusted Inference Engine: Preventing Neural Network Exfiltration in Hardware Devices*, Department of Electrical and Computer Engineering, McCormick School of Engineering, Northwestern University, 2018.
Host Dr. Valerie Taylor	*Secure Execution of Neural Network Accelerators*, Mathematics and Computer Science (MCS) division, Argonne National Laboratory, 2018.
Host Prof. Houman Homayoun	*Designing Secure Heterogeneous Multicore Systems from Untrusted Hardware and Software Components*, Department of Electrical and Computer Engineering, George Mason University, 2018.
Host Prof. Sherief Reda	*Designing Secure Heterogeneous Multicore Systems from Untrusted Components*, ECE Department, Brown University, 2017.
Workshop | 2017	*Secure Architecture Design*, 3rd Career Workshop for Women and Minorities in Computer Architecture - 50th IEEE/ACM International Symposium on Microarchitecture (MICRO-50), 2017.
Host Prof. V. Joyner Koomson	*A Scalable Asynchronous Architecture for Fast Processing of Large Graph Applications*, ECE Department, Tufts University, 2017.
Host Prof. Pengju Ren	*Asynchronous Architecture Design for Fast Processing of Large Graph Applications*, Institute of Artificial Intelligence and Robotics, Xi'an Jiaotong University, 2017.
Host Prof. Leibo Liu	*Self-Aware Polymorphic Computer Architecture Design*, Institute of Microelectronics, Tsinghua University, 2017.
Host Prof. Marten van Dijk	*Cyber-Physical Systems Security: Wearable and Implantable Devices*, ECE Department, University of Connecticut, 2016.
CyberSEED Conference	*Secure Heterogeneous Multicore Architecture Design*,Comcast Center of Excellence for Security Innovation, University of Connecticut, 2016.
Seminar	*Fast Processing of Large Graph Applications Using Asynchronous Architecture*, MIT LL Cyber Operations, Research and Engineering (CORE) Seminar Series - Division 5 , 2016.

Host Prof. Ronald Metoyer — *Secure Multicore Architecture Design*, ECE Department, University of Notre Dame, 2016.

Workshop — *Secure Multicore Architecture Design,*, Pacific Northwest Workshop on Securing Hardware Design and IC Supply Chains, sponsored by Mentor Graphics, Intel, and Galois, 2016.

Host Antonio de la Serna — *Cognitive-Approximate Architectures*, Draper Laboratory, 2015.

Workshop — *Hardware Level Computer Systems Security*, Oregon Cyber Security Day, University of Oregon, 2015.

Host Serge Leef — *Augur: A software-hardware co-design framework for efficient execution of binary code diversification*, Mentor Graphics, 2015.

Host Prof. Christof Teuscher — *MARTHA: A Cyber-Physical System Domain Architecture*, ECE Department, Portland State University, 2014.

Host Prof. Ronald Metoyer — *Adaptive and Polymorphic Computer Architectures*, ECE Department, Oregon State University, 2014.

Recent Invited Panelist

NYU — *MARTHA: A Cyber-Physical System Domain Architecture*, ECE Department, Portland State University, 2014.

CLSAC — *Adaptive and Polymorphic Computer Architectures*, ECE Department, Oregon State University, 2014.

Major Software Released

Trireme RISC-V — Open Source Architectural Design Space Exploration Toolbox around the RISC-V ISA (Link: `https://www.trireme-riscv.org/`.

Gauge — An Interactive Machine Learning-Driven Knowledge Extraction, Analysis and visualization Tool (Link: `https://www.gaugeviz.org/index.html`.

Q-Effect — Open-Source FPGA Implementation of Post-Quantum Cryptographic Hardware Primitives (Link: `https://ascslab.org/research/pqcp/index.html`.

ABAQS — Agent Based Architecture for Quorum sensing Simulation (Link: `http://ascslab.org/research/abc/abaqs/index.html`.

Heracles — A Tool for Fast RTL-Based Design Space Exploration of Multicore Processors (Link: `http://projects.csail.mit.edu/heracles/`.

Research Activities

Major Research Sponsors

External — Department of Defense (DOD)/Air Force Research Laboratory

External — Department of Defense (DOD)/National Security Agency

External	Department of Defense (DOD)/Air Force Material Command
External	Defense Advanced Research Projects Agency (DARPA)
External	Department of Energy (DOE)
External	Sandia National Laboratories
External	Argonne National Laboratory
External	Brookhaven National Laboratory
External	MIT Lincoln Laboratory
External	National Science Foundation (NSF)
External	Altera Corporation - Equipment and software licenses
External	Xilinx Corporation - Equipment and software licenses
External	Intel Corporation - Equipment

Service

PROFESSIONAL SERVICE TO COMMUNITY

Broadening Participation

- *University of the Virgin Islands Summer Cybersecurity Program*: This summer training introducing students to hardware approaches to cybersecurity. The students gain in-depth introduction to the role that hardware plays in cybersecurity and computer hardware related attacks and defense in computing systems.

- *ASCS Laboratory Summer Digital Design Program*: The summer program is six-week hands-on course that teaches digital design, memory operation, memory-based attacks and hardware modifications to protect against memory corruption using a field-programmable gate array (FPGA) toolkit.

- *Tapia Conference Secure Computer Systems Design Workshops*: For the past three years, two workshops have been introduced to the Tapia conference - one is called "Next-Generation Secure Computer Systems - Post-Quantum Cryptosystems" and the other "BRISC-V: A RISC-V Open-Source Architecture Design Space Exploration Toolbox".

ACADEMIC INTERNAL SERVICE

Department Level.

2021 - 2022	School of Computing and Augmented Intelligence (SCAI), Arizona State University, School Director Search Committee
2020 - 2021	School of Computing and Augmented Intelligence (SCAI), Arizona State University, Faculty Search Committee
2020 - 2022	School of Computing and Augmented Intelligence (SCAI), Arizona State University, PhD Program Committee
2017 - 2020	Department of Electrical and Computer Engineering, Boston University, Masters Program Committee

2016 - 2018 Department of Electrical and Computer Engineering, Boston University, Faculty Search Committee

2016 - 2017 Department of Electrical and Computer Engineering, Boston University, PhD Program Committee

2015 - 2016 Dept. of Computer and Information Science, University of Oregon, Graduate Education Committee

2014 - 2016 Dept. of Computer and Information Science, University of Oregon, Computing Resources Committee

2014 - 2015 Dept. of Computer and Information Science, University of Oregon, Colloquium Chair

College Level.

2016 - 2017 College of Engineering, Future of Undergraduate Engineering Education Task Force

University Level.

2018 - 2019 Recruitment Committee of Boston University

2015 - 2016 University of Oregon, Incubating Interdisciplinary Initiatives (I3) Review Committee

2014 - 2016 University of Oregon, Regional Accelerator and Innovation Network at UO Advisory

2014 - 2016 University of Oregon, University Venture Development Fund program - Leadership Team

ACADEMIC EXTERNAL SERVICE

Conference Organizing Committee.

2022 International Symposium on Computer Architecture (**ISCA**)

2022 USENIX Security Symposium (**USENIX**)

2020 ACM Richard Tapia Celebration of Diversity in Computing (**TAPIA**)

2019 ACM Great Lakes Symposium on VLSI (**GLSVLSI**), Co-Organizer of Special Session: Approximate Computing Systems Design: Energy Efficiency and Security Implications?

2019 24rd ACM International Conference on Architectural Support for Programming Languages and Operating Systems(**ASPLOS**) Publicity Co-Chair.

2018 IEEE International Conference on Computer Design (**ICCD**) Registration Co-Chair.

2018 IEEE Computer Society Annual Symposium on VLSI (**SVLSI**), Co-Organizer of Special Session: Shall We Jointly Address VLSI Reliability and Security?

2017 50th Annual IEEE/ACM International Symposium on Microarchitecture (**MICRO-50**) Registration Chair.

2017 IEEE Symposium on Neuromorphic Cognitive Computing (**SNCC**), Co-Organizer of Special Session: Design Methods, Tools and Examples for FPGA-Based Acceleration of Artificial Neural Network.

Workshop Organizing Committee.

2020 International Symposium on Performance Analysis of Systems and Software (**ISPASS**), Founder and Organizer for the First International Workshop on Secure RISC-V Architecture Design - SECRISC-V 2020 Workshop

2019 Boston Area Architecture 2019 Workshop, (**BARC18**) General Co-Chair.

Conference Track Chair.

2020 IEEE/ACM International Conference on Computer-Aided Design (**ICCAD**).
Track 1.7 Security Architecture and System

2020 IEEE International Midwest Symposium on Circuits and Systems (**MWSCAS**).
10 Hardware Security

Conference Session Chair.

2018 IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**).
Session 2: Physical Attacks and Tamper Resistance

2017 IEEE International Conference on Computer Design (**ICCD**).
9B: Novel Architecture with 3D and Flash Memory

2017 60th IEEE International Midwest Symposium on Circuits and Systems (**MWSCAS**).
11.2 Trusted Microelectronics Track

Conference Review Committee.

2020 IEEE International Symposium on Workload Characterization (**IISWC**)

2020-2021 Design Automation Conference (**DAC**)

2019, 2021 International Symposium on Computer Architecture (**ISCA**)

2019, 2020 International Symposium on High Performance Computer Architecture (**HPCA**)

2018 - 2020 IEEE/ACM International Conference on Computer-Aided Design (**ICCAD**).

2018 IEEE International Conference on High Performance Computing, Data, and Analytics (**HiPC**).

2018, 2019 Asian Hardware Oriented Security and Trust Symposium (**AsianHOST**).

2018, 2019 IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**).

2018 - 2020 ACM Great Lakes Symposium on VLSI (**GLSVLSI**).

2016 - 2020 IEEE High Performance Extreme Computing (**HPEC**).

2017, 2022 IEEE/ACM International Symposium on Microarchitecture **MICRO-50**).

2017 International Conference for High Performance Computing, Networking, Storage and Analysis (**Supercomputing - SC**) - Architectures and Networks Program Committee.

2015 - 2017 IEEE International Conference on Computer Design (**ICCD**).

2017, 2018 IEEE International Midwest Symposium on Circuits and Systems (**MWSCAS**).

2017 IEEE International Parallel and Distributed Processing Symposium (**IPDPS**).

2015 ACM Richard Tapia Celebration of Diversity in Computing Conference.

Journal Review Committee.

2018-2019 IEEE Transactions on Very Large Scale Integration Systems (**TVLSI**).

2016-2019 ACM Transactions on Reconfigurable Technology and Systems (**TRETS**).

2016-2021 IEEE Transactions on Computers (**TC**).

2016 IEEE Transactions on Parallel and Distributed Systems (**TPDS**).

2018, 2016 ACM Transactions on Architecture and Code Optimization (**TACO**).

Grant Review Panels.

2014-2021 Department of Defense External Reviewer.

2019-2020 National Science Foundation Proposals.

2015 US Department of Energy SBIR Proposals.

Professional Memberships

Institute of Electrical and Electronics Engineers (IEEE).

Association for Computing Machinery (ACM).

Miscellaneous

Citizenship: **United States**

References

Available upon request.